HADMÉRNÖK

Kiemelt közlemények

21. évf. (2026)
1. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9–11.
Postacím: 1581 Budapest, Pf. 15.
„A” épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000/29-289, Fax: +36-1-432-9025
E-mail: hadmernok@uni-nke.hu
Web: https://folyoirat.ludovika.hu/index.php/hadmernok

Kiadó
Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes

Tartalom

Védeleminformatika

Környezetbiztonság

Fórum

Katonai logisztika

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 1. szám 5–24.
DOI: 10.32567/hm.2026.1.1

Dániel Griffiths[1]

Analysing Cognitive-Computing-Based Countermeasures to Cyber Threats against Critical Infrastructures

Abstract

Critical infrastructures are vital to the functioning of modern societies but are increasingly exposed to sophisticated cyber threats due to heightened convergence of information technology and operational technology environments. The inherent complexity and presence of legacy components within these systems significantly expand the attack surface, making traditional security measures insufficient. This work analyses the evolving threat landscape facing critical infrastructures and presents a comprehensive assessment of cognitive computing-based countermeasures. Emphasising recent advances in cognitive computing, the article explores adaptive defence mechanisms capable of evolving alongside emerging threats. The analysis highlights the effectiveness and limitations of these approaches, their applicability within cyber-physical systems, and their potential to bridge gaps between IT and OT security. Ultimately, the research underscores the importance of integrating these techniques into cybersecurity strategies to enhance the resilience of critical infrastructure systems.

Keywords: cognitive computing, machine learning, cybersecurity, critical infrastructure, cyber-physical systems

The attack surface of critical infrastructures

Critical infrastructures play a vital role in the functioning of modern societies, ensuring the smooth operation of everyday life. These infrastructures are generally defined as the totality of physical and virtual assets, systems and services whose failure, destruction, or prolonged disruption could have a serious, widespread impact, threatening

[1] PhD student, Óbuda University, Doctoral School on Safety and Security Sciences.

the safety of the population, the functioning of the state and the stability of the economy. As a result, attacks against critical infrastructures may have profound societal, economic and national security implications. A successful attack may disrupt daily life, economic activity or even public order. Furthermore, the targeting of strategic services such as energy, communications, or transport systems can impede governmental functioning and threaten national sovereignty.[2]

Modern critical infrastructures are highly interconnected and interdependent, so much so that an attack on a single component may trigger cascading effects across multiple systems.[3] Advanced attacks against cyber-physical systems can cause long-term damage, undermine system reliability, and demand substantial financial resources for recovery.[4] High-profile incidents may also generate social panic and erode public confidence in institutions, thus contributing to long-term societal destabilisation.[5] These risks necessitate the prioritisation of critical infrastructure within national cybersecurity strategies, yet effective defence is hindered by the complexity and limited transparency of such systems.

The ongoing digitisation of industrial environments has further intensified these challenges. The cyber-physical systems typically found in critical infrastructures differ significantly from traditional IT systems and operate under very different constraints. These difficulties are compounded by the legacy nature of many critical infrastructures, a significant portion of which was constructed in the mid-20th century or even earlier.[6] Such systems were originally designed as closed, physically isolated environments, with security based primarily on obscurity rather than true cyber resilience.[7] Increased connectivity has since exposed these systems to modern threats, while industrial control system (hereinafter ICS) manufacturers historically placed limited emphasis on cybersecurity, relying on proprietary protocols and physical isolation as protective measures.[8] Consequently, many known vulnerabilities remain unpatched due to unsupported operating systems, long lifecycles and stringent operational requirements.[9] Continuous operation and high availability constraints further limit opportunities for modernisation, patching and security testing, given the severe societal and economic consequences of service interruptions.[10] These technical challenges are exacerbated by the relative specialisation of cyber-physical system security and a persistent shortage of skilled cybersecurity professionals, which disproportionately affects the resilience of critical infrastructures.[11]

A central challenge in defending critical infrastructures is the exposure created by external attack surfaces, which arise primarily at interfaces connecting infrastructure components to public or less controlled networks. In many cases, such systems are

[2] Riggs et al. 2023; Lis–Mendel 2019; Haig–Kovács 2012.
[3] Palleti et al. 2021; Wang et al. 2018.
[4] Baezner–Robin 2017; Jermalavičius et al. 2025.
[5] Tabansky 2011.
[6] Osei-Kyei et al. 2021.
[7] Assenza et al. 2020.
[8] Hurst–Shone 2024; Daricili–Çelik 2022.
[9] Wilson 2014.
[10] Booth et al. 2019; Assenza et al. 2020.
[11] ISC2 2024; ISACA 2024.

inadvertently exposed due to misconfiguration or inadequate network segmentation.[12] Industrial control systems are especially vulnerable, as internet-connected devices can be rapidly identified using automated search engines such as Shodan, enabling targeted attacks.[13] These systems frequently lack robust authentication and encryption, thus creating trivially simple opportunities for unauthorised access, traffic interception or manipulation.[14]

Attackers commonly exploit vulnerable services and open ports associated with outdated, improperly configured, or unpatched software, using automated discovery and exploitation tools. Well-documented attacks against critical cyber-physical systems, such as Stuxnet,[15] Industroyer[16] and Triton,[17] demonstrate how adversaries can gain initial access through exposed interfaces or insufficiently protected remote access and subsequently perform data theft, system manipulation, or physical sabotage. The rapid proliferation of industrial Internet of Things devices further expands the external attack surface, as direct connectivity to cloud-based management platforms introduces additional attack vectors when connections are inadequately secured.[18]

A further major source of risk arises from the exploitation of trusted relationships. Rather than targeting critical infrastructures directly, adversaries may compromise less protected partners, suppliers or service providers from the target's supply chain.[19] These attacks exploit established trust relationships based on routine data exchange, software updates, remote management, or certificate-based authentication. Software supply chain attacks are particularly dangerous where critical infrastructures rely on widely used software or third-party components that are regularly updated. By compromising a software developer or distributor, attackers can inject malicious code into legitimate update mechanisms, which are then automatically deployed by operators who trust the source. Such attacks are difficult to detect, as they abuse valid digital signatures and legitimate distribution channels.

Trusted relationships also arise from interoperability and permissive access arrangements between interconnected systems.[20] Critical infrastructures often operate multiple integrated networks with shared connectivity or authentication mechanisms, enabling attackers who compromise a less secure subsystem to pivot into more sensitive environments. These trust-based connections can produce cascading breaches, allowing a single compromise to undermine multiple layers of defence. The risks associated with this are further exacerbated by increasing reliance on third-party services such as remote maintenance and cloud-based monitoring.[21]

Cyberattacks against critical infrastructure are not limited to technical exploitation, but frequently rely on human manipulation or physical intrusion. Despite the

12 Leszczyna–Egozcue 2013.
13 Wilson 2014.
14 Leszczyna–Egozcue 2013.
15 MITRE Corporation 2025.
16 MITRE Corporation 2024a.
17 MITRE Corporation 2024b.
18 Hurst–Shone 2024.
19 Hurst–Shone 2024.
20 Leszczyna–Egozcue 2013.
21 Hurst–Shone 2024.

deployment of technical safeguards, the human element remains a critical vulnerability.[22] Social engineering attacks exploit such weaknesses by manipulating individuals into disclosing sensitive information, granting unauthorised access or performing actions that undermine operational security. Attackers may impersonate trusted figures such as IT personnel, managers, or external partners, subsequently coercing users into compromising their credentials or systems and enabling undetected access to sensitive resources.

Insider threats present a related risk, where individuals with legitimate access may intentionally or unintentionally facilitate breaches due to negligence, coercion, financial incentives or personal grievances. Such actors can misuse authorised privileges to exfiltrate data, sabotage systems or assist external adversaries. These threats are particularly concerning in critical infrastructure environments, given their strategic importance and the potential involvement of foreign actors seeking to undermine national security. Insider attacks are difficult to mitigate because they exploit trust-based organisational structures and access controls that are essential for normal operations.

Physical breaches constitute a distinct but closely related threat vector. Direct physical attacks aim to disrupt or destroy infrastructure components through forceful means, producing immediate and severe consequences that require significant recovery efforts. More sophisticated cyber-physical attacks leverage physical access to enable digital compromise rather than outright destruction.[23] Attackers may gain entry under the guise of maintenance or contracting activities and introduce infected devices into restricted or air-gapped networks. By bridging physical and digital domains, such hybrid operations circumvent conventional cybersecurity measures based on network isolation or remote-access controls, and their physical appearance may obscure the underlying objective of covert digital infiltration.

Research goals and methodology

Taking into account the threat landscape detailed earlier, the primary objective of this paper is to explore the applicability and potential effectiveness of cognitive computing solutions for the protection of cyber-physical systems present in critical infrastructures. One area of focus is the comparative assessment of the cybersecurity maturity of critical infrastructures with traditional IT environments. Building on these differences, one aim of the study is to analyse the extent to which cognitive defensive solutions applied in traditional IT environments can be adapted to critical infrastructure environments and how they could potentially address the previously identified attack surfaces. The research also aims to identify relevant cognitive approaches that are conceptually suitable for responding to complex threats to cyber-physical systems and provide a scientific basis for further targeted research directions.

[22] Ghafir et al. 2018.
[23] Loukas 2015.

The research methodology is built around a literature review approach, with the objective of assessing cognitive computing approaches in the context of critical infrastructure protection. This involved identifying the relevant research areas, along which a structured keyword-based search strategy could be employed. The review draws on peer-reviewed academic publications as well as industry reports to ensure that the analysis covers both theoretical and practical aspects. The search process focused primarily on the most recent and relevant work, which was complemented by the historical sources necessary to understand the conceptual background. The analysis focuses on approaches that are empirically grounded and applicable to cyber-physical environments. The review thematically categorises these approaches and performs a comparative analysis, allowing for the systematic identification of research challenges, current practices, as well as perceived technological and conceptual gaps.

Existing cognitive-computing-based countermeasures

Cognitive computing represents a new generation of information systems that can simulate aspects of human thinking using approaches such as artificial intelligence (hereinafter AI) and the closely related field of machine learning (hereinafter ML). These systems do not simply follow pre-programmed logic, but learn from their environment and make real-time decisions based on information learned from complex data sets.

Over the past decade, these approaches have undergone significant development, driven by digitisation, automation, and the recognition of the economic and innovation potential of generative AI. Cognitive systems are gradually emerging in IT security, enabling more sophisticated defensive measures and supporting the automation of complex tasks. Although their use in protecting cyber-physical systems in critical infrastructures is still in its infancy, cognitive computing offers particularly promising opportunities, and a number of studies have begun investigating how these systems can help address the specific types of threats targeting these environments. The following sections discuss the research areas that have begun investigating the potential use cases for this technology in the field of critical infrastructures.

Network traffic analysis

Traditional signature-based systems use known attack patterns (signatures) to identify threats to cyber-physical systems (hereinafter CPS), meaning they can only detect predefined threats and are thus ineffective against unknown (zero-day) attacks. In contrast, machine learning-based anomaly detection models the normal behaviour of the system and identifies deviations from it as potential attacks. Their advantage is that they do not require prior signatures; are able to adapt to a variety of CPS systems; and can operate with unlabelled data in unsupervised learning, which is particularly useful in volatile and complex CI environments. Over the past decade, there has been a significant increase in the number of research projects dealing with

ML-based anomaly detection for CPSs and CI. Since the early 2010s, there has been a steady increase in the number of publications, mainly in the fields of computer science and engineering, reflecting the multidisciplinary security challenges of CPS/CI systems and the growing importance of cognitive approaches.[24]

There are numerous cognitive computing approaches in the field of network traffic analysis and intrusion detection, all of which essentially rely on some form of machine learning technique. The chosen learning paradigm significantly influences detection capabilities, especially when dealing with challenges such as zero-day attacks, data drift, and issues of scalability and generalisability.

One such research project investigated the detection of malicious CPS network traffic using a range of classical machine learning and deep learning approaches.[25] The tests involved various classification tasks, where k-nn and decision tree models were tested alongside deep learning approaches such as CNN-LSTM architectures. Based on the researchers' results, these approaches provide virtually error-free predictions on the data sets used. The data set chosen by the authors did not contain any "exploit-like" attacks, thus protection against zero-day attacks is questionable and questions remain about the robustness and generalisability of the resulting systems.

A different research article underpins the idea that deep learning is highly effective for intrusion detection in CPS environments.[26] The presented reinforcement learning model demonstrated strong performance on two industrial IoT datasets, particularly in detecting attacks such as port scans and false command injections. Although the study achieved excellent accuracy, the question still remains regarding the types and number of attacks present in the training datasets, as well as the fact that the study did not include a confusion matrix for each attack category, which makes it difficult to determine how robust the protection is (e.g. in the case of zero-day attacks).

There has also been research exploring the possibilities of unsupervised learning, focusing on the problem of zero-day attack detection. This approach uses machine learning algorithms trained only on data representing normal system functionality. These models are then used to identify deviations from this learned baseline. Such systems appear promising with one paper finding the model capable of identifying 23 out of 26 attack scenarios in a real-world accurate dataset.[27] Similar approaches have been proposed using semi-supervised anomaly detection mechanisms that deviate from the earlier previously mentioned unsupervised models by being also trained with a small amount of labelled data. This method also showed positive results in handling zero-day threats, with the added benefits of low false positive rates.[28]

In addition to the research described above, there are numerous other promising research results that suggest that we are talking about a mature field of research that is already working on ironing out late-stage problems.[29] The main open issue left is generalisability and adaptability to zero-day attacks. This could primarily be achieved

[24] Rouzbahani et al. 2020.
[25] Alkahtani–Aldhyani 2022.
[26] Mesadieu et al. 2024.
[27] Pinto et al. 2024.
[28] Vávra et al. 2021.
[29] Pinto et al. 2023.

by producing more comprehensive data sets that place greater emphasis on zero-day-like attacks and exploits and better represent the real network traffic experienced in critical infrastructures. However, the production of such public datasets that reflect real-world environments may continue to raise significant national security concerns and therefore may remain limited.

Research has been published recommending the use of large language models (hereinafter LLMs) to detect network anomalies in critical infrastructure.[30] These may seem particularly promising in less sensitive IT environments, but in systems where the security of critical infrastructure is at stake, it is essential that security teams have complete sovereignty over both their data and the models into which they feed it. With API-based integrations, there is a risk that data of national security importance could fall into the wrong hands, either directly or indirectly (e.g. through third-party cloud-based systems). Even in case of locally run LLMs, the "black box" nature of the models raises serious concerns, particularly with regard to the exact data used to train them. It cannot be ruled out that nation state actors have deliberately introduced poisoned data sets into publicly available training data, which could result in the model's behaviour being not only unpredictable but also deliberately manipulated.

Automated threat hunting

Another promising research direction using cognitive computing is automated threat hunting. One such research article presented a threat hunting architecture that integrates machine learning methods and visualisation techniques to protect critical infrastructures.[31] The system they propose collects and normalises information from SIEMs, log files, PCAP data and OSINT sources to identify suspicious behaviours.

At the core of the system is an anomaly detection mechanism that uses various machine learning algorithms to identify deviations from previously observed normal behaviour in the infrastructure. Methods such as clustering techniques, decision-tree-based approaches and various neural network architectures work together to achieve this goal. These algorithms are capable of highlighting unusual events from log files or network traffic, recognising multi-step, hidden attack patterns, and learning from new data and threat hunter feedback to increasingly accurately distinguish between benign and malicious behaviour. Natural language processing modules enable the system to extract contextual and semantic information from unstructured sources such as analyst reports, incident descriptions, or threat intelligence materials, and combine this with detected activities to further increase detection accuracy. A novel feature of the system is the hypothesis generator module, which uses the results of various machine learning outputs and rule-based filters to generate attack hypotheses and perform probability assessments, enabling automatic prioritisation of incidents. The system is capable of learning responses to recurring, benign events and treating

[30] Markevych–Dawson 2023.
[31] Aragonés et al. 2023.

them with lower priority, thereby bringing new or rare, potentially dangerous behaviours to the forefront.

Although the technical structure and operating mechanism of the system are well thought out, the publication does not detail exactly what types of anomalies the model is capable of detecting, which raises questions about its practical applicability. During validation in a digital twin-based test environment, the authors found that the system was capable of processing large data streams in real time, detecting complex attacks and integrating expert feedback. After six months, the proportion of events correctly classified as harmless increased to 83.49%, while the attack detection rate increased to 86.31%. However, the article does not provide detailed information on the types of attacks detected or the environment in which the system was tested (e.g. the industry or technological background of the infrastructure), which makes it difficult to assess the validity and generalisability of the results.

In another study with a similar goal but a different approach, the authors presented a proactive threat hunting method that uses multiple machine learning algorithms to detect suspicious activities that may occur in critical infrastructures.[32] The outlined approach is more similar to a traditional anomaly detection machine learning algorithm than to the previous true threat hunting-based approach. Similarly to threat hunting in a traditional SIEM system, this approach is akin to using queries that are too noisy to be actual alert rules, but can still reveal genuine malicious activity.

This approach therefore uses a number of machine learning algorithms to detect suspicious activities, which can then be investigated manually by human analysts. The system was tested on open-source bank transaction data to detect attacks against banking systems (mainly targeting SWIFT). Certain classification approaches achieved high accuracy rates of up to 95.7%, but based on the confusion matrices shown in the research, the false negative rate is quite high. It is also important to consider how applicable these results are in practice. A noisy threat hunting query in a SIEM system provides interpretable results, as the underlying logic is transparent, allowing an analyst to continue the investigation. In contrast, with a machine learning-based approach, where the decision logic is completely opaque, an analyst will not know with certainty how to investigate the case further. Therefore, further research is needed on the validity of such approaches, especially in comparison with the hypothesis-based approach outlined earlier.

Behavioural biometrics

As explained at the beginning of this article, compromised users and internal threats pose a serious challenge to the protection of critical infrastructure. A defence mechanism for this can be found in the areas of advanced behaviour analysis, anomaly detection and behavioural biometrics.

[32] Shan–Myeong 2024.

One such approach is a deep learning-based authentication method that analyses users' keystroke dynamics.[33] This approach introduces a novel method in the field of keystroke dynamics behavioural biometrics, which is capable of converting numerical temporal features into visual representations. This allows users' password entry patterns to be evaluated in visual form, enabling the detection of subtle behavioural differences using a Siamese convolutional neural network, which can be used to distinguish the original user from a potential insider attacker.

During the training of the model, it learns to keep the embeddings of samples from the same user close to each other, while placing samples from different users far apart in the multidimensional representation space. A significant advantage of the methodology presented in this research is that it can identify users not only in the case of static, predefined passwords, but also across different passwords and password lengths. The approach was validated using multiple datasets and metrics, and although there are significant fluctuations in accuracy from dataset to dataset (84.0% to 99.2%), the solution demonstrates significant potential for detecting compromised authentication data.

This level of behavioural biometrics and anomaly detection allows us to detect password compromise after a social engineering or phishing attack if the input pattern differs from that of the legitimate user. It is conceivable that with further research, insider threats will also be detectable using similar approaches, as similar non-critical infrastructure-specific research already exists.[34] This would allow the detection of data leaks or the issuance of malicious PLC commands based on keystrokes. A sufficiently sophisticated model could potentially even identify users who have been deceived by social engineering and are acting under duress.

Sensor fusion

Cognitive computing-based methods also play a role in enhancing the physical security of critical infrastructures. One such example has achieved promising results using applied multimodal data fusion and adaptive deep learning approaches.[35] The authors propose an attack detection framework that combines visual surveillance data, Wi-Fi channel state information, and PLC/SCADA sensor data in a machine learning classification framework. This multimodal approach achieves significantly better detection performance than any unimodal approach, as demonstrated by detailed experimental results in the publication.

The test data set was recorded as part of the EU Horizon 2020 STOP-IT project, a research initiative for the protection of critical water infrastructure, in which eight water utility companies participated as consortium members. The dataset covers various data sources, including video streams from security cameras, Wi-Fi signal data, and data from industrial control systems. The ICS sensor data comes from

[33] Budžys et al. 2024.
[34] Wang et al. 2018; Bondada–Bhanu 2014.
[35] Bakalos et al. 2019.

the SCADA systems of real-world water infrastructure and includes the suction and discharge pressure values of two pumps and data on the water level in a water tank. The data was labelled based on predefined scenarios jointly defined by the water utility operators. These labels can be classified into four main categories.

- normal operation
- cybersecurity attacks (targeting ICS systems)
- physical intrusions (including suspicious movements in protected areas, monitored using RGB and thermal cameras)
- cyber-physical attacks consisting of a combination of the above approaches

The solution proposed by the research is a TDL–CNN architecture that is capable of analysing temporal precedents, so that detection results take into account not only current data but also data from hundreds of previous points in time. This reduces false alarms and increases robustness in dynamically changing attack environments where threats can be physical, cyber or a combination. The results are promising, reaching an accuracy of up to 87.62%. Given the high dimensionality and volume of the data, even better results may be achievable by applying newer neural network architectures more suited to multimodal large datasets. In addition, the use of camera data is likely to improve the interpretability of alerts, as this visual information gives security teams an accurate idea of when an attack occurred and what systems were accessed.

Unimodal approaches, primarily using visual data, may also have their place in protecting critical infrastructures. Use cases where visual anomaly detection can identify physical damage may be useful for surveillance and remote monitoring use cases. Although comprehensive research for uses is limited, there have been proposals for using machine learning-based classification algorithms for powerline inspections.[36] The authors in this case only aimed to classify tower types and did not attempt to detect damage or other abnormalities. However, with further development of this approach, the identification of manipulated, damaged towers or foreign objects could also be turned into a visual multi-class classification problem. Further development of the method, for example by adding multimodal sensor fusion outlined earlier (e.g. using Lidar), could further improve sabotage detection capabilities.

Analysis and future research

As discussed in previous sections, the cybersecurity of critical infrastructure has become one of the most important challenges of the digital age. However, this area still does not receive the attention it deserves in research and development involving cognitive computing techniques. While the use of cognitive computing to enhance the cybersecurity of information technology systems has long been an active area of research, research on industrial and operational technologies is much less common. The current lack of prioritisation is not only risky but also irrational, as most IT research could be adapted to critical infrastructure with minor modifications.

[36] Sampedro et al. 2014.

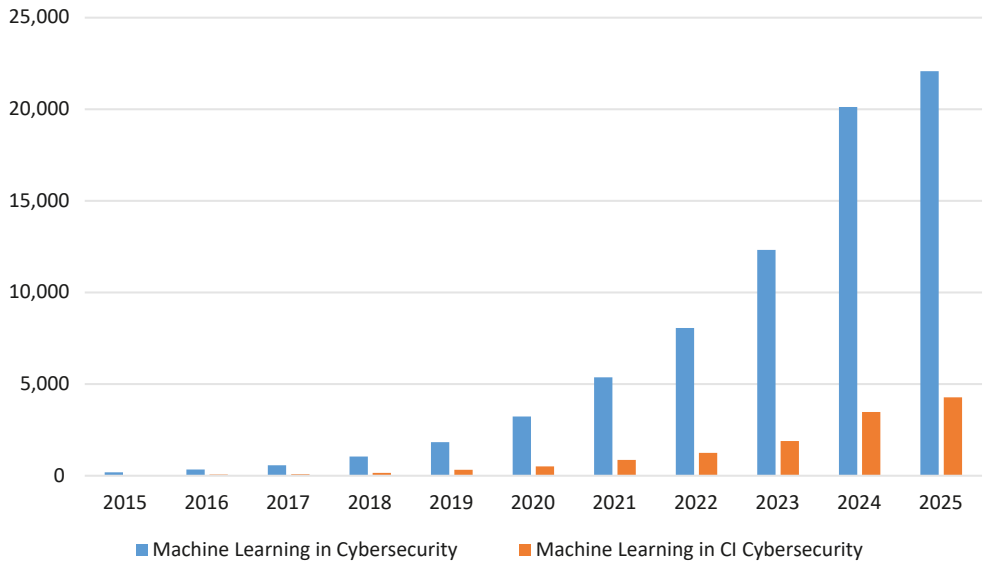


Figure 1: Disparity in machine learning-related Scopus indexed articles
Source: compiled by the author

One of the fundamental reasons why OT cybersecurity does not receive enough attention is the previously established operating paradigm, according to which these systems were physically isolated from IT networks and were closed, proprietary environments optimised primarily for availability as well as secure operation in harsh industrial conditions. As a result, organisations may view OT systems as not requiring the same level of security attention as IT infrastructures. However, this attitude is becoming increasingly untenable.

Technological advances and industry competition are driving ever greater IT/OT convergence, with increased interconnectivity between the two networks. This has made real-time data collection, remote control, and advanced analytics available in systems that previously operated in isolation. IT/OT convergence is further accelerated by the demand for production optimisation, predictive maintenance and centralised management, as well as the proliferation of cloud-based solutions.

As a result, OT systems are moving towards more open, interoperable architectures and integrating more IT-based technologies into their operations.[37] Parallel to the technical and operational convergence of IT and OT systems, it would be logical for security research in both areas to be mutually applicable. Many principles and methodologies, such as access management, network segmentation and incident detection can be adapted from the IT environment to the OT domain, especially in newer, more open systems. Future cybersecurity research should therefore aim to bridge the artificial divide between IT and OT and promote knowledge transfer between the two domains, particularly in the protection of critical infrastructure. Therefore,

[37] Leszczyna–Egozcue 2013.

in the following sections, several approaches using IT-specific cognitive computing techniques are presented and related areas for potential development are explored, which could be applied to the cyber-physical environments of critical infrastructures.

Ensuring network segmentation

The application of machine learning-based network segmentation in information technology networks is a method that already exists and is supported by research.[38] The essence of this approach is that, instead of traditional manual segmentation, large amounts of passively collected IP traffic data is used to automatically form behaviour-based network segments, which can then be separated from each other using firewall or routing rules. IP flow-based network monitoring allows for the collection of metadata from a large volume of traffic at a single central measurement point without direct access to the hosts. This connection-oriented data requires further processing to be transformed into host-oriented behaviour profiles.

During behaviour-based segmentation, features are first selected from the IP flow data that describe the network behaviour of individual hosts. These may include: the number of traffic connections belonging to a host, the number of bytes and packets communicated, the number of peers reached, used ports, protocols and their hourly trends. From these characteristics, a large-scale temporal behaviour pattern is formed for each host.

The authors tested the automated segmentation using several machine learning algorithms, particularly clustering techniques. The research shows that in behaviour-based clustering, the number of actually distinct behavioural clusters is usually much smaller than the number of segments created on an organisational (administrative units) basis, as devices with identical or similar functions often belong to different administrative groups but have similar network behaviour. However, if the subset under investigation exhibits well-distinct behavioural patterns, behaviour-based clustering can show a near-perfect alignment with well-designed logical segments.

Another main application of machine learning segmentation is assigning unknown hosts to existing segments. Here, classification algorithms (primarily clustering algorithms) are used, which assign the host to the most suitable segment based on its behaviour profile. These methods are most accurate (up to 92%) when the behaviour of the segments is well differentiated, while in case of administrative segments, where host behaviour often overlaps, accuracy is around 50–60%.

In principle, this approach could be directly adapted to industrial control technology environments. OT systems are characterised by a narrower set of protocols and traffic that is often more deterministic than in IT networks, which means that behaviour-based profiling could be even more effective. The advantage of the IP flow-based approach is that it does not require the installation of agents on sensitive OT devices, and traffic data can be collected at the edge of the network, thus increasing visibility while maintaining system integrity. Classifying individual OT devices into

[38] Smeriga–Jirsik 2019.

segments and automatically classifying new or unknown devices can significantly contribute to refining segmentation rules while adapting to dynamic changes in the OT network. This reduces the network attack surface and limits lateral movement in the event of a successful attack.

Generative AI for deception

Honeypots based on generative artificial intelligence are a new type of cyber deception tools that leverage the capabilities of LLMs or generative pre-trained transformer models to provide realistic interactive responses to attackers while avoiding the typical limitations of traditional honeypots.[39] These systems are capable of simulating text-based interactions, such as command line terminals or even complete protocols, where the generative model responds to every incoming command or request based on the current context and history of the system. Prompt engineering techniques allow the model's "personality" and context to be precisely defined, such as to mimic a specific operating system, device, or service. To make responses more deterministic, the input prompt and context can be continuously and dynamically edited to ensure the realism and consistency of outputs.

The key to the operation of generative AI honeypots is that when an attacker's command or interaction is received, the system pre-processes the input through a so-called front-end interface layer and then post-processes the response given by the model (e.g. filtering sensitive information or self-disclosing outputs), and finally returns it to the adversary. Context management plays a critical role in ensuring that only command-response pairs that actually modify the state of the system are retained, while the entire command history can be optionally stored for special cases (e.g. history commands). This significantly reduces token usage and increases response coherence, enabling longer, more convincing attacker sequences to be handled without hitting the LLM's token limits.

The use of such honeypots seems feasible in CPS environments, as they could allow simulating the behaviour of industrial control systems, PLCs, DCSs, or even IoT/IIoT devices in the form of textual or protocol-level interactions. By customising the prompt or potentially with some limited model retraining or fine tuning, a generative AI honeypot has the potential to simulate an industrial protocol or interpret and respond to a command set similar to that of a specific PLC. Through its adaptive capabilities, the model could respond to new, previously unseen attack patterns and dynamically expand the simulated behaviour patterns based on attacker interactions, thus avoiding rapid fingerprinting of static honeypots. In addition, this approach minimises the risk of the attacker breaking out of the honeypot, as they cannot execute real code on the backend system.

On the other hand, generative AI honeypots are likely to face a number of technical challenges, especially in OT environments. The determinism of LLMs is only partially guaranteed. Due to the stochastic selection of tokens, different responses

[39] Ragsdale–Boppana 2023.

may be generated for the same command, which could expose deception to a persistent attacker. During long or complex sequences, hallucinations may occur or the token limit can be quickly reached if the entire history of every interaction is always passed to the model. These problems may be solvable by using various prompt and context management and post-processing techniques. Furthermore, the binary protocol-level communication often used by real OT systems can only be simulated to a limited extent with text-based models. Therefore, generative AI honeypots must be combined with other traffic generation tools, or special generative models must be created with unique data sets that are capable of simulating these binary protocols.

Software supply chain monitoring

As discussed in previous sections, supply chain attacks pose a serious threat to industrial control systems, where attackers can cause physical damage or compromise operations by installing malicious or faulty control code. Code analysis could play a key role in preventing and detecting such attacks, as it allows potential vulnerabilities, logical errors, or unwanted functions to be identified before installation, even without running the code.

However, current methods of code analysis for cyber-physical systems, especially in OT/ICS environments, rarely use cognitive computing approaches. Instead, traditional static code analysis techniques are used for formal or semantic analysis of industrial control programmes. These methods typically first translate PLC programmes into an intermediate representation (hereinafter IR) that contains simple instructions such as assignments, jumps and conditional branches.[40] This IR normalises the different PLC languages, making them uniformly analysable. Next, a control flow graph is created from the IR, which depicts the possible execution paths of the programme. Abstract interpretation is then performed on this graph, during which the value ranges of each variable in the programme are assigned to the various possible execution branches. Based on this data, predefined rules and checks are executed to identify syntactic errors, potential runtime errors, unwanted variable values, or even dangerous logical branches. Such static analyses are suitable for detecting when a malicious or otherwise flawed code snippet could cause dangerous behaviour. However, these methods often generate a large number of false positives because they cannot take into account the runtime context, such as whether parts of the code are actually accessible during real operation or how the physical environment limits possible execution paths. Furthermore, such static rule-based approaches are limited or unable to detect unknown weaknesses, such as zero-day vulnerabilities or attack vectors that were not originally considered by the developers. In contrast, machine learning-based approaches are typically more generalisable and can therefore be more effective against unknown attacks.

In other areas, such as classic information technology systems or software development processes, cognitive computing and code analysis approaches are already

[40] Stattelmann et al. 2014; Zonouz et al. 2014; Zhang et al. 2019.

widespread.[41] These systems were typically trained with large amounts of source code, machine code, binaries, configuration files, or even documentation elements and use ML algorithms, including various specialised language processing techniques. Similar to classical approaches, the first step in AI/ML-based code analysis is typically the production of an intermediate representation of the source code, such as an abstract syntax tree, control flow graph or simple tokenisation, followed by feature extraction. The machine learning model then classifies or predictively evaluates the code snippets, for example, by predicting whether a given code snippet contains vulnerabilities, backdoors, anomalies, or other undesirable behaviour.

LLMs offer a new perspective on detecting these software vulnerabilities. Not only are these models capable of understanding the syntactic and semantic structure of source code, but by learning from a huge codebase, they implicitly incorporate various programming patterns and contexts related to previous vulnerabilities.[42] Such an approach enables LLMs to automatically identify and determine which input points in a given software project represent potential threats and which API calls or functions are the locations where improperly sanitised data could cause security vulnerabilities. This not only increases the effectiveness of vulnerability detection, but also significantly reduces false positives, especially when LLMs are able to decide on the relevance of an issue by taking into account the context of the entire project. Furthermore, the use of LLMs offer even greater potential for discovering new or previously unknown vulnerabilities, as the models are able to generalise based on the vast amount of learned patterns and recognise correlations that traditional ML models may not be capable of. These AI-based analysers may enable significant automation of large-scale software system audits or even detect hidden, sophisticated attacks, especially if they are able to learn from past attack patterns, such as the characteristics of supply chain malware.

Machine learning-based static code analysis can offer significant advances in the protection of cyber-physical systems, especially when integrated into continuous integration processes, where fast, automated and reliable decision-making is critical. Such approaches allow a dedicated ML-based verification step to identify potentially problematic patterns before code or updates are deployed, potentially enabling early detection of zero-day vulnerabilities. In the automatic analysis of supplier code, this type of method is not only suitable for searching for specific defects, but may also be capable of filtering out suspicious components based on broader behavioural patterns. This significantly reduces the risk of intentional tampering, before the code is deployed in a production environment.

Conclusion

The increasing digitisation, interconnectivity, and convergence of information technology and operational technology environments have significantly expanded the

[41] Wang et al. 2021.
[42] Li 2025.

cybersecurity attack surface of critical infrastructures. Legacy systems, which were often designed without robust security considerations, are now exposed to sophisticated and evolving cyber-physical threats with potentially severe societal, economic and national security implications. Due to the multifaceted nature of cyber-physical systems, traditional security approaches are proving inadequate, creating a growing potential for countermeasures based on cognitive computing. Despite this potential, their practical application within CIs remains limited and lags behind their more mature application in traditional IT domains.

A key obstacle to the advancement of cognitive security solutions in OT environments is the scarcity of representative, real-world datasets possibly due to national security concerns. This limits the generalisability, adaptability and robustness of existing models, especially in detecting zero-day attacks, coping with protocol diversity and the complex operational characteristics of CPS. Although multiple approaches have shown high accuracy, challenges persist in maintaining low false positive rates and extending detection capabilities to encompass a broader range of physical and hybrid attack vectors.

Additionally, while much of the existing cognitive-computing-based security research has been developed in IT environments, these methodologies often rely on open architectures and large-scale data infrastructures that are not typically found in critical infrastructure environments. Nevertheless, with appropriate adaptations, these approaches offer valuable insights and technological foundations that can be transferred to CPS systems, particularly as the boundary between IT and OT continues to blur.

Future research should prioritise bridging the gap between IT and OT cybersecurity by adapting proven IT-based cognitive computing approaches to the distinct requirements of critical infrastructure. This entails developing robust, privacy-preserving datasets, enhancing model interpretability, and creating context-aware systems tailored to the physical and operational constraints of CIs. Promoting interdisciplinary integration between IT and OT domains is critical to implementing secure, resilient and adaptive defence strategies for critical infrastructures.

References

Alkahtani, Hasan – Aldhyani, Theyazn H. H. (2022): Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems. *Electronics,* 11(11), 1–25. Online: https://doi.org/10.3390/electronics11111717

Aragonés, Mario Lozano – Llopis, Israel Pérez – Domingo, Manuel Esteve (2023): Threat Hunting Architecture Using a Machine Learning Approach for Critical Infrastructures Protection. *Big Data and Cognitive Computing,* 7(2), 1–26. Online: https://doi.org/10.3390/bdcc7020065

Assenza, Giacomo – Faramondi, Luca – Oliva, Gabriele – Setola, Roberto (2020): Cyber Threats for Operational Technologies. *International Journal of System of Systems Engineering,* 10(2), 128–142. Online: https://doi.org/10.1504/IJSSE.2020.109127

Baezner, Marie – Robin, Patrice (2017): *Hotspot Analysis: Stuxnet.* Zürich: Center for Security Studies, 1–16. Online: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Bakalos, Nikolaos – Voulodimos, Athanasios – Doulamis, Nikolaos – Doulamis, Anastasios – Ostfeld, Avi – Salomons, Elad – Caubet, Juan – Jimenez, Victor – Li, Pau (2019): Protecting Water Infrastructure from Cyber and Physical Threats: Using Multimodal Data Fusion and Adaptive Deep Learning to Monitor Critical Systems. *IEEE Signal Processing Magazine,* 36(2), 36–48. Online: https://doi.org/10.1109/MSP.2018.2885359

Bondada, Mahesh Babu – Bhanu, S. Mary Saira (2014): Analyzing User Behavior Using Keystroke Dynamics to Protect Cloud from Malicious Insiders. *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),* 1–8. Online: https://doi.org/10.1109/CCEM.2014.7015481

Booth, Adrian – Dhingra, Aman – Heiligtag, Sven – Nayfeh, Mahir – Wallance, Daniel (2019): *Critical Infrastructure Companies and the Global Cybersecurity Threat.* New York: McKinsey & Company. Online: www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/critical%20infrastructure%20companies%20and%20the%20global%20cybersecurity%20threat/critical-infrastructure-companies-and-the-global-cybersecurity-threat-vf.pdf?shouldIndex=false

Budžys, Arnoldas – Kurasova, Olga – Medvedev, Viktor (2024): Deep Learning-based Authentication for Insider Threat Detection in Critical Infrastructure. *Artificial Intelligence Review,* 57(10), 1–35. Online: https://doi.org/10.1007/s10462-024-10893-1

Daricili, A. Burak – Çelik, Soner (2022): National Security 2.0: The Cyber Security of Critical Infrastructure. *Perceptions: Journal of International Affairs,* 26(2), 259–276. Online: https://dergipark.org.tr/en/download/article-file/2181981

Ghafir, Ibrahim – Saleem, Jibran – Hammoudeh, Mohammad – Faour, Hanan – Prenosil, Vaclav – Jaf, Sardar – Jabbar, Sohail – Baker, Thar (2018): Security Threats to Critical Infrastructure: The Human Factor. *The Journal of Supercomputing,* 74(10), 4986–5002. Online: https://doi.org/10.1007/s11227-018-2337-2

Haig, Zsolt – Kovács, László (2012): Kritikus infrastruktúrák és a kritikus információs infrastruktúrák elleni fenygetettségek, támadások. In Ványa, László (ed.): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest: Nemzeti Közszolgálati Egyetem, 92–167.

Hurst, William – Shone, Nathan (2024): Critical Infrastructure Security: Cyber-threats, Legacy Systems and Weakening Segmentation. In Tekinerdogan, Bedir – Akşit, Mehmet – Catal, Cagatay – Hurst, William – Alskaif, Tarek (eds.): *Management and Engineering of Critical Infrastructures.* Cambridge, Mass.: Academic Press, 265–286. Online: https://doi.org/10.1016/B978-0-323-99330-2.00010-6

ISACA (2024): *State of Cybersecurity 2024. Global Update on Workforce Efforts, Resources, and Cyberoperations.* Schaumburg: ISACA. Online: www.isaca.org/resources/reports/state-of-cybersecurity-2024

ISC2 (2024): *Global Cybersecurity Workforce Prepares for an AI-Driven World.* Alexandria: ISC2. Online: https://edge.sitecorecloud.io/internationf173-xmc4e73-prod-

bc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf

Jermalavičius, Tomas – Rõigas, Henry – Sukhodolia, Oleksandr – Teperik, Dmitri (2025): *The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector.* Tallinn: International Centre for Defence and Security. Online: https://icds.ee/wp-content/uploads/dlm_uploads/2025/05/ICDS_Report_The_Staying_Power_of_Ukrainian_Lights_Jermalavicius_Roigas_Sukhodolia_Teperik_May_2025.pdf

Leszczyna, Rafal – Egozcue, Elyoenai (2013): ENISA Study: Challenges in Securing Industrial Control Systems. In Laing, Christopher – Badii, Atta – Vickers, Paul (eds.): *Securing Critical Infrastructures and Critical Control Systems. Approaches for Threat Protection.* Hershey: IGI Global, 105–143. Online: https://doi.org/10.4018/978-1-4666-2659-1.ch005

Li, Ziyang – Dutta, Saikat – Naik, Mayur (2025): LLM-Assisted Static Analysis for Detecting Security Vulnerabilities. *ArXiv,* 1–24. Online: https://doi.org/10.48550/arXiv.2405.17238

Lis, Piotr – Mendel, Jacob (2019): Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review,* 5(2), 24–47. Online: https://doi.org/10.18559/ebr.2019.2.2

Loukas, George (2015): *Cyber-Physical Attacks. A Growing Invisible Threat.* Newton: Butterworth-Heinemann. Online: https://doi.org/10.1016/B978-0-12-801290-1.00011-4

Markevych, Michal – Dawson, Maurice (2023): A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI). *International Conference, The Knowledge-Based Organization,* 29(3), 30–37. Online: https://doi.org/10.2478/kbo-2023-0072

Mesadieu, Frantzy – Torre, Damiano – Chennamaneni, Anitha (2024): Leveraging Deep Reinforcement Learning Technique for Intrusion Detection in SCADA Infrastructure. *IEEE Access,* 12, 63381–63399. Online: https://doi.org/10.1109/ACCESS.2024.3390722

MITRE Corporation (2024a): *Industroyer.* Online: https://attack.mitre.org/software/S0604/

MITRE Corporation (2024b): *Triton.* Online: https://attack.mitre.org/software/S1009/

MITRE Corporation (2025): *Stuxnet.* Online: https://attack.mitre.org/software/S0603/

Osei-Kyei, Robert – Tam, Vivian – Ma, Mingxue – Mashiri, Fidelis (2021): Critical Review of the Threats Affecting the Building of Critical Infrastructure Resilience. *International Journal of Disaster Risk Reduction,* 60, 1–11. Online: https://doi.org/10.1016/j.ijdrr.2021.102316

Palleti, Venkata Reddy – Adepu, Sridhar – Mishra, Vishrut Kumar – Mathur, Aditya (2021): Cascading Effects of Cyber-attacks on Interconnected Critical Infrastructure. *Cybersecurity,* 4, 1–19. Online: https://doi.org/10.1186/s42400-021-00071-z

Pinto, Andrea – Herrera, Luis-Carlos – Donoso, Yezid – Gutierrez, Jairo A. (2023): Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors,* 23(5), 1–18. Online: https://doi.org/10.3390/s23052415

Pinto, Andrea – Herrera, Luis-Carlos – Donoso, Yezid – Gutierrez, Jairo A. (2024): Enhancing Critical Infrastructure Security: Unsupervised Learning Approaches for Anomaly Detection. *International Journal of Computational Intelligence Systems,* 17, 1–18. Online: https://doi.org/10.1007/s44196-024-00644-z

Ragsdale, Jarrod – Boppana, Rajendra V. (2023): On Designing Low-Risk Honeypots Using Generative Pre-Trained Transformer Models with Curated Inputs. *IEEE Access,* 11, 117528–117545. Online: https://doi.org/10.1109/ACCESS.2023.3326104

Riggs, Hugo – Tufail, Shahid – Parvez, Imtiaz – Tariq, Mohd – Khan, Mohammed Aquib – Amir, Asham – Vuda, Kedari Vineetha – Sarwat, Arif I. (2023): Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors,* 23(8), 1–26. Online: https://doi.org/10.3390/s23084060

Rouzbahani, Hossein Mohammadi – Karimipour, Hadis – Rahimnejad, Abolfazl – Dehghantanha, Ali – Srivastava, Gautam (2020): Anomaly Detection in Cyber-Physical Systems Using Machine Learning. In Choo, Kim-Kwang Raymond – Dehghantanha, Ali (eds.): *Handbook of Big Data Privacy.* Cham: Springer, 219–235. Online: https://doi.org/10.1007/978-3-030-38557-6_10

Sampedro, Carlos – Martinez, Carol – Chauhan, Aneesh – Campoy, Pascual (2014): A Supervised Approach to Electric Tower Detection and Classification for Power Line Inspection. *2014 International Joint Conference on Neural Networks (IJCNN),* 1970–1977. Online: https://doi.org/10.1109/IJCNN.2014.6889836

Shan, Ali – Myeong, Seunghwan (2024): Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors,* 24(15), 1–24. Online: https://doi.org/10.3390/s24154888

Smeriga, Juraj – Jirsik, Tomas (2019): Behavior-Aware Network Segmentation Using IP Flows. *14th International Conference on Availability, Reliability and Security (ARES 2019),* 1–9. Online: https://doi.org/10.1145/3339252.3339265

Stattelmann, Stefan – Biallas, Sebastian – Schlich, Bastian – Kowalewski, Stefan (2014): Applying Static Code Analysis on Industrial Controller Code. *2014 IEEE Emerging Technology and Factory Automation (ETFA),* 1–4. Online: https://doi.org/10.1109/ETFA.2014.7005254

Tabansky, Lior (2011): Critical Infrastructure Protection against Cyber Threats. *Military and Strategic Affairs,* 3(2), 61–78. Online: www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1326273687.pdf

Vávra, Jan – Hromada, Martin – Lukáš, Luděk – Dworzecki, Jacek (2021): Adaptive Anomaly Detection System Based on Machine Learning Algorithms in an Industrial Control Environment. *International Journal of Critical Infrastructure Protection,* 34, 1–11. Online: https://doi.org/10.1016/j.ijcip.2021.100446

Wang, Jingjing – Huang, Minhuan – Nie, Yuanping – Li, Jin (2021): Static Analysis of Source Code Vulnerability Using Machine Learning Techniques: A Survey. *2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD),* 76–86. Online: https://doi.org/10.1109/ICAIBD51990.2021.9459075

Wang, Weiping – Yang, Saini – Hu, Fuyu – Stanley, H. Eugene – He, Shuai – Shi, Mimi (2018): An Approach for Cascading Effects within Critical Infrastructure Systems. *Physica A: Statistical Mechanics and its Applications,* 510, 164–177. Online: https://doi.org/10.1016/j.physa.2018.06.129

Wang, Xuebin – Tan, Qingfeng – Shi, Jinqiao – Su, Shen – Wang, Meiqi (2018): Insider Threat Detection Using Characterizing User Behavior. *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC),* 476–482. Online: https://doi.org/10.1109/DSC.2018.00077

Wilson, Clay (2014): Cyber Threats to Critical Information Infrastructure. In Chen, Thomas M. – Jarvis, Lee – Macdonald, Stuart (eds.): *Cyberterrorism.* New York: Springer, 123–136. Online: https://doi.org/10.1007/978-1-4939-0962-9_7

Zhang, Mu – Chen, Chien-Ying – Kao, Bin-Chou – Qamsane, Yassine – Shao, Yuru – Lin, Yikai – Shi, Elaine – Mohan, Sibin – Barton, Kira – Moyne, James – Mao, Z. Morley (2019): Towards Automated Safety Vetting of PLC Code in Real-World Plants. *2019 IEEE Symposium on Security and Privacy (SP),* 522–538. Online: https://doi.org/10.1109/SP.2019.00034

Zonouz, Saman – Rrushi, Julian – McLaughlin, Stephen (2014): Detecting Industrial Control Malware Using Automated PLC Code Analytics. *IEEE Security & Privacy,* 12(6), 40–47. Online: https://doi.org/10.1109/MSP.2014.113

HADMÉRNÖK
VÉDELEMINFORMATIKA

21. évfolyam (2026) 1. szám 25–39.
DOI: 10.32567/hm.2026.1.2

Zoltán Kovács[1]

The Use of Artificial Intelligence in Cyberattacks, Part 3

Phases 5–7 (+1) of the Cyber Kill Chain Model, Challenges, Trends, Outlook

Abstract

The first part of the series of articles provided a basic understanding of the fundamental concepts of artificial intelligence and its relevant subfields, and demonstrated that the Cyber Kill Chain (CKC) model is suitable for achieving the main objective of the article, despite all its limitations, i.e. it can be used to review what AI-supported tools attackers can already use in the various phases of a cyberattack and how these tools help them. The second part of the series examined the latter in phases 1–4 of the CKC, while this article, the third part of the series, shows how attackers can use AI in the last three plus one phases of the CKC and how it helps them achieve their goals. In addition, this article highlights the challenges attackers face when using AI and presents the trends that can be observed in cyberattacks. Finally, this article makes recommendations for the direction of further research, namely, to examine the possibilities of using AI-supported defence solutions in the individual phases of CKC and to compare the possibilities of the attacking and defending sides in order to develop effective response capabilities.

Keywords: artificial intelligence, cybersecurity, cyberattack, Cyber Kill Chain, C2, maintaining a persistent presence, exfiltration, system disruption

Introduction

The second part of this series of articles examined how attackers can use AI in phases 1–4 of the Cyber Kill Chain (CKC) model and how it helps them achieve their goals. One of the main findings of this article was that although in 2024, major cybersecurity companies still wrote in their annual studies that attackers typically rely on artificial

[1] Senior Lecturer, Ludovika University of Public Service, e-mail: zkovacs.24@gmail.com

intelligence in the first two phases of the CKC, i.e. reconnaissance and weaponisation, based on an examination of the first four phases, it can be said that over the past 1.5–2 years, with the development of AI, its malicious use has also advanced significantly. This can be measured in several ways. On the one hand, attackers have further refined previously known AI-assisted attack methods, making them even more effective. Examples include the production of extremely realistic deepfake content and the preparation and execution of convincing phishing attacks that bridge language gaps and are written with perfect grammar. On the other hand, AI support has also appeared in forms of attack that were previously unknown or only marginally encountered and were therefore little known to defenders. Examples include the integration of defence evasion techniques into malicious code, the creation of polymorphic[2] and metamorphic[3] malware, intelligent exploit generation, autonomous exploit execution and optimisation, and even AI support for acoustic side-channel attacks.

Based on the above, it can be concluded that if so many new developments have occured in the past 1.5–2 years, even in the early stages of CKC, when the forms of AI support for attacks and their usage were more familiar, then it is worthwhile to continue the research and examine the AI-supported attack options used by attackers in the later stages of CKC. The third part of this series of articles examines the current possibilities available to attackers in the last three (plus one) phases of CKC if they wish to use AI-supported tools for their attacks and shows how these tools can help attackers achieve their goals. It examines the challenges and trends that are emerging in the use of AI in attacks and then makes recommendations for the direction of further research.

The application of AI in the individual phases of the Cyber Kill Chain

The capabilities of artificial intelligence, and thus its use, significantly enhance attackers' capabilities in cyberattacks, enabling them to accelerate, automate and refine their execution. The second part of this series of articles presented in detail how attackers could utilise artificial intelligence in the first four phases of the CKC (i.e. the cyberattack chain) and what specific technologies they could use to achieve their malicious goals. This article examines the last three (plus one) phases of the CKC from the same perspective.

[2] Polymorphic malware: malicious software that can change its own code with each infection in order to make it more difficult to detect by traditional defence tools, such as antivirus software. Polymorphic malware changes its original code so that each time it infects a system, it has a different, unique code fragment and binary code structure, while its malicious function remains unchanged. Malware often includes a mutation engine that automatically generates new encryption keys and algorithms (ITszótár.hu 2025).

[3] Metamorphic malware: in addition to the characteristics of polymorphic malware, it is also capable of changing, rewriting, translating and editing its own code, so that each new version differs from the previous one, all without using an encryption key. This is a more advanced technique than polymorphic malware, which uses a key to modify the code. Metamorphic malware is more difficult to detect and identify because its code is constantly changing, it has no constant part that would identify it, and it does not return to its original form; each distributed version differs from the previous one. This rewriting may involve changing the order of the code, adding unnecessary instructions (so-called *garbage code*), or replacing existing instructions with instructions that have equivalent functionality but different code (ITszótár.hu 2025).

Phase 5: Installation

After successful exploitation, the installation phase follows. In this phase, the attacker installs malicious software (e.g. backdoor, rootkit, virus) to ensure a persistent presence on the compromised system. AI can help attackers here, for example by automating the installation of backdoors and helping to maintain a persistent hidden presence.[4]

- *Malware configuration, installation and privilege escalation:* AI can help attackers not only in creating the malware they use, but also in installing it, configuring it during operation, and obtaining higher privilege levels. They are able to collect system information, search key folders of the operating system, dynamically control malware, etc. AI can also facilitate privilege escalation, for example by using LLM design to generate exploit chains. These allow attackers to penetrate deeper into the network after the initial intrusion, install the prepared malicious code, and then be able to execute their final goal.[5]
- *Rootkit and bootkit*[6] *optimisation:* AI can optimise rootkits (malware hidden deep within the system that conceals its presence and activity, allowing attackers to access compromised machines and the data stored on them undetected) and bootkits (malware that compromises the system boot process, load before the operating system, and are able to mask their presence from the operating system and the applications installed on it, such as security software for example, antivirus programmes). This is because AI is capable of recognising kernel-level security mechanisms and making modifications to the malicious code that are least likely to trigger alarms from security devices and software, thus ensuring a persistent, deeply embedded presence in the compromised system.[7]
- *Hidden file system operations and defence against forensic investigations:* AI can help malware successfully installed on the target system to maintain a persistent presence and achieve its goals by performing the necessary operations on the file system (e.g. creating or modifying files, manipulating system logs or metadata) that leave as little digital footprint as possible. This can make it significantly more difficult to detect malicious activity and identify the source of the attack. This capability significantly increases the ability to maintain the hidden nature of attacks and makes it difficult to identify attackers.[8]
- *Intelligent, persistent presence maintenance mechanisms:* AI can analyse the target system configuration, installed software and user accounts in order to select the least detectable and most resistant mechanisms for the malicious code to maintain its presence. With the help of AI algorithms, malware can learn which registry keys, scheduled tasks, services, or file system modifications appear the least suspicious, and can automatically adapt if defence systems detect and

[4] Darktrace 2024.
[5] De Pasquale et al. 2024; Toulas 2025.
[6] A rootkit or bootkit is a malicious code that inserts itself into the boot process of a computer and is able to perform operations that would not be permitted by the operating system.
[7] Kewat 2025; Lee et al. 2025.
[8] Jain–Chhabra 2014; Pappachan et al. 2024.

attempt to remove them. AI can analyse the target system's configuration, installed software, and user accounts in order to select the least detectable and most resilient mechanisms for the malicious code to maintain its presence. With the help of AI algorithms, malware can learn which registry keys, scheduled tasks, services, or file system modifications appear the least suspicious, and can automatically adapt if defence systems detect and attempt to remove them. Factors such as the self-modifying capabilities of malware (polymorphic and metamorphic malware), the use of obfuscated code, the generation of false telemetry or log data to evade defence tools, the use and maintenance of persistent, multiple backdoors against system reboots or authentication changes, or the use of fileless malware techniques, as described earlier, also contribute to maintaining a persistent presence. In addition, AI-driven malware may be able to repair itself if certain components are deleted or if the persistence points necessary for its continued existence are modified.[9]

Based on the above, it can be said that AI can help increase the effectiveness of attacks even in the fifth phase of the CKC, i.e. the installation phase. AI enables malicious software to become more autonomous and resilient, gain higher privileges more quickly, and evade security measures, making it difficult to remove and ensuring its persistent presence within the compromised network. This attack capability also strengthens the necessity to shift the defence paradigm from relying on static signatures to AI-supported behavioural analysis and continuous monitoring to detect and eliminate advanced threats.

Phase 6: Command and Control (C2)

In the Command and Control (C2) phase of CKC, the attacker establishes an encrypted and hidden communication channel with the malware installed on the compromised system, enabling remote control and data exfiltration from the target system. AI enables autonomous management of C2 channels, allowing the malware to operate independently. The AI-controlled use of the C2 channel can dynamically adapt to network defences, thereby increasing the resilience of C2 communications against detection and helping to maintain a persistent connection between the control server and the malicious code running on the target system.[10]

- *Adaptive and covert C2 communications:* AI-based C2 modules are capable of dynamically changing their communication patterns (e.g. protocols, ports, timings, data formats) in order to avoid detection by security systems during network traffic analysis. With the help of machine learning (ML), the C2 agent can learn which network traffic patterns appear legitimate on a given network (e.g. web browsing, DNS queries, cloud-based services, etc.) and can blur or embed malicious communications within them. For example, AI-driven

[9] Schröer et al. 2025.
[10] Lockheed Martin s. a.; Powell 2025.

C2 modules may be capable of using automatic Domain Generation Algorithms (DGA), which, on the one hand, evaluate and classify DNS queries from compromised hosts using the Generative Adversarial Networks[11] (GANs) already mentioned in the previous article, and on the other hand, generate a large number of rapidly changing domain names, making it significantly more difficult for defence systems to effectively filter them out using blacklists. But AI-supported C2 modules are also capable of hiding C2 communications by embedding them in legitimate protocols using steganography. This makes it difficult or impossible for defence systems to detect such communications, as C2 communications are more difficult to track or, if detected, more difficult to block.[12]

- *Decentralised and flexible C2 infrastructure:* AI can help attackers manage the distributed and dynamically changing C2 infrastructure they create, which is more resistant to disconnections and blockages, enabling them to carry out effective attacks. AI can autonomously switch C2 servers as needed, use peer-to-peer (P2P) networks, or embed C2 capabilities into legitimate cloud services (e.g. Google Drive, Dropbox, etc.), making it significantly more difficult to detect and neutralise the attacker's infrastructure. AI-controlled botnets are capable of building and maintaining highly adaptive and difficult-to-eliminate C2 infrastructure, which they can use to launch extremely sophisticated, coordinated, and targeted attacks with unpredictable or difficult-to-predict appearances, changes and further evolution.[13]
- *Intelligent detection avoidance during network traffic monitoring:* The AI components controlling C2 communications may be able to learn from the operation of network anomaly detection systems (NADS). This includes the use of adversarial machine learning techniques, where AI makes minimal modifications to the communication pattern that are just enough to outsmart the defensive AI models, but do not interfere with the C2 functionality used for the attack.[14]

In summary it can be said that AI also plays a significant role in the command-and-control phase of CKC, where it can greatly assist attackers in achieving their objectives. AI enables the development, operation and maintenance of more covert, adaptive and autonomous C2, can reduce the digital footprint left behind by attackers, and can increase resistance to the activities of defenders.

[11] GANs consist of two neural networks (generator and discriminator) that compete with each other and ultimately produce better output (results) than if only one network were operating and providing results for a given question or task.
[12] Powell 2025; Anderson et al. 2016.
[13] Wang et al. 2022; Frisoni 2020.
[14] Abbadi–Lachkar 2024; Wang et al. 2023.

Phase 7: Actions on Objectives

This is the final phase of the Cyber Kill Chain, where the attacker achieves the ultimate goals of the attack. AI can significantly increase the effectiveness of the attack in this phase, as well as its speed or, in some cases, its destructive potential. AI can also effectively support the evasion of defence systems (e.g. dynamic malware behaviour) and, in the case of ransomware, it can help estimate the value of data, but it can also automate the collection of additional authentication data required for access, lateral movement, or the destruction or wiping of data in the target system and the disabling of systems.[15]

- *Optimised exfiltration:* AI can also help attackers by automatically identifying the most valuable and sensitive data within the network (e.g. intellectual property, personal data, financial information, critical configuration files, etc.), prioritise the information marked for acquisition, and optimise the routes and timing of the data to be exfiltrated so that the exfiltration of the data can be as inconspicuous as possible. To circumvent anomaly detection used on compromised networks, AI can use reinforcement learning to find out what network bandwidth usage or data packet size is considered normal and then *regulate* the extraction of the desired data accordingly.[16]
- *Intelligent execution of DDoS attacks and adaptation to defensive operations:* AI-based distributed denial-of-service (DDoS) botnets are capable of adapting in real time to defence mechanisms and changes in the infrastructure of their victims. AI can learn which attack vectors (e.g. volumetric targeting the network layer, application-level targeting the application layer) are most effective against a given target and dynamically modify the type of attack, traffic intensity, or source IP address rotation to achieve maximum results.[17]
- *Automated ransomware management:* AI can accelerate either the spread of ransomware within a compromised network or its operation, i.e. the encryption of data on target machines, by automating the identification of the most valuable files and systems that are worth encrypting for the attacker. AI-based chatbots are able to automate negotiations with ransomware victims based on a profile of the victim previously prepared with the help of AI, optimising the amount of ransom that can be obtained and the payment deadlines for the attacker, while minimising the manual effort required by the attackers. The use of AI-based chatbots further reduces the risk of the attacker being caught, as in the event of a possible *red-handed* arrest, the police will only find machines and not people.[18]
- *System disruption and integrity damage:* As mentioned earlier, AI can help attackers identify critical system components and/or data within a compromised network. This not only helps attackers extract or encrypt data, but can also optimise destructive operations (e.g. deleting data, disabling systems,

[15] Microsoft Security 2025.
[16] Al-Azzawi et al. 2025; Aboze 2025.
[17] Sangfor Technologies 2025; Utter 2024.
[18] Cherepanov–Strýček 2025; Trinckes s. a.

modifying firmware, etc.). All this is done in a way that causes the greatest possible damage while making it difficult for defenders to recover quickly. AI may also be able to develop strategies to maximise chaos, such as preparing operations aimed at disrupting recovery processes or damaging the integrity of backups, and may even be able to assist in their execution.[19]

Overall, it can be said that even in the final phase of CKC, i.e. the action on objectives, AI can significantly assist attackers in carrying out cyberattacks. The use of AI accelerates and optimises the final stage of a cyberattack by maximising the damage caused and financial gain, while minimising the time available for defenders to detect and respond. This means that the impact of successful intrusions is likely to be more severe and widespread.

Summary of AI use in the seven phases of Cyber Kill Chain

Based on the above, it can be said that the use of artificial intelligence in each phase of the Cyber Kill Chain significantly enhances the capabilities of attackers, automates, accelerates, and refines cyberattacks. Table 1 below summarises the use of AI in each phase of the CKC.

Table 1: The application of AI in the phases of the Cyber Kill Chain – Summary

CKC phase	**Main objective of the CKC phase**	**AI-enhanced attack capabilities and abilities**	**AI sub-branches that can be used for attacks**
1. Reconnaissance	Gathering information about the target	• Automated OSINT • Target profiling • Network mapping • Vulnerability detection • Human behaviour analysis • Data recovery from acoustic signals	ML, NLP, DL
2. Weaponisation	Preparation of malicious tools (exploit + payload)	• AI-based malware generation (polymorphic/metamorphic) • Exploit selection • Intelligent exploit generation • Generation of content that can be used for personalised social engineering attack • Integration of defence evasion techniques	Generative AI (GANs, LLMs), RL, DL, NLP
3. Delivery	Delivery of cyber weapons to their target	• Optimised delivery channels and timing • Delivery hiding • Automated password cracking • Execution of intelligent phishing campaigns • Supply chain attacks	ML, Generative AI, NLP

[19] Boutin 2025; Raz et al. 2025.

CKC phase	Main objective of the CKC phase	AI-enhanced attack capabilities and abilities	AI sub-branches that can be used for attacks
4. Exploitation	Exploiting vulnerabilities to gain access	• Independent exploit execution and optimisation • Application of intelligent defence evasion techniques • Application of polymorphism and metamorphism	RL, ML, DL
5. Installation	Providing persistent presence on the compromised system	• Malware configuration, installation, privilege escalation • Rootkit/bootkit optimisation • Hidden file system operations and defence against forensic investigations • Intelligent persistence mechanisms	ML, Adversarial ML
6. Command and Control (C2)	Establishment of encrypted communication channels	• Adaptive and hidden C2 communication • Decentralised and flexible C2 infrastructure • Avoidance of detection during network traffic monitoring	ML, Adversarial ML
7. Actions on Objectives	Achievement of the ultimate objectives of the attack	• Optimised data exfiltration • Execution of intelligent DDoS attacks • Automated ransomware management • System destruction	ML, RL

Source: compiled by the author

Phase +1: Monetisation

Although the monetisation phase is not part of Lockheed Martin's original model, many experts have added it to the model. Phase +1 focuses on the attacker's activities to monetise the information obtained from a successful attack. AI can also optimise processes and assist attackers in this phase.[20]

Ransomware and ransom payments: AI can assist attackers not only in creating and distributing ransomware, but also in managing ransom payments for stolen data and conducting negotiations themselves.[21]

Selling data on the dark web: AI can help evaluate and sell stolen data on the dark web, thereby optimising profits for attackers.[22]

Fraud and financial manipulation: AI-driven fraud, such as financial fraud committed using deepfakes (e.g. fake CEO calls), can cause significant financial losses. AI-based systems such as FraudGPT are capable of creating personalised business email compromise (BEC) emails and fraudulent websites, increasing their credibility and the success rate of social engineering attacks.[23]

[20] Microsoft Security 2025.
[21] Holden 2023.
[22] Tejedor 2025.
[23] Humphries 2026.

Overall, it can be concluded that phase +1 of CKC is closely related to the previous phases, as most of the elements described above have already appeared in them. At the same time, it is worth focusing on the possibilities described here during defence planning, i.e. it may be worthwhile to look outside the protected networks, to the dark web, in order to break or track attacks. Of course, in certain cases, defenders will need to seek the help of the appropriate authorised organisations (e.g. the police), which may again be an advantage for attackers.

Challenges and trends in the use of AI in cyberattacks

The above series of articles has shown how attackers can use AI in the various phases of a CKC and how it can increase the effectiveness of an attack. It can therefore be concluded that the use of AI in cyberattacks heralds new trends and, at the same time, significant challenges. However, these new challenges do not only affect defence professionals, but also pose significant problems for attackers, requiring serious consideration on their part. It can be argued that the use of AI will become indispensable on the offensive side, given the need to increase the effectiveness of attacks and the spread of evolving AI-based defence tools. In addition, competition is also expected to increase among attackers, as those who use AI-supported solutions will be more successful and able to obtain more information and thus more money.

At the same time, in addition to the challenges, thanks to the rapid development of AI, significant new opportunities will emerge in the near future that could further enhance the effectiveness of attackers. At the end of this series of articles, it is worth reviewing these opportunities alongside the challenges in order to be even better prepared for defence.

Challenges in applying AI in attacks

As explained above, although AI offers enormous opportunities for attackers, they may encounter a number of obstacles when carrying out sophisticated AI-based attacks. These challenges typically include the following:

- *Computing resources required for AI:* Running and training advanced AI models, especially deep learning and reinforcement learning systems, requires significant computing resources (primarily specialised hardware with multiple GPU cards) and energy consumption. This can hinder and significantly limit the capabilities of average or less well-funded attack groups. At the same time, *AI-as-a-Service* (AIaaS) platforms and easy and relatively inexpensive access to cloud-based computing resources can significantly reduce this barrier, making these advanced attack capabilities available to the aforementioned attack groups with less capital.[24]

[24] Timilehin 2023; Mailchimp s. a.

- *Data quality and quantity:* The effectiveness of AI models depends largely on the quality and quantity of the data used for training. The accuracy, completeness, consistency, and timeliness of the latter are essential for AI to work effectively. In other words, data quality has a critical impact on the performance of machine learning models. AI models trained and operating on poor-quality, incomplete, or distorted data may be insufficiently effective or produce poor-quality results that are easily detectable by defenders. This can make it difficult for attackers to collect a sufficient amount of relevant data that is appropriate for their purposes to train targeted AI models.[25]
- *Attribution and traceability:* Although AI-driven attacks make it significantly more difficult for defenders to understand and trace attacks due to dynamically changing infrastructure and automated decision-making, this can also cause difficulties for attackers. This is because it can be challenging for them to fully control and track the behaviour of their own AI systems used for attacks. Losing control can lead to unwanted side effects during the attack. In such cases, attackers' AI tools may leave digital footprints (e.g. specific characteristics of the AI model used, patterns derived from training data, etc.) that defenders may be able to detect and even trace back.[26]
- *The AI arms race between attackers and defenders:* The increasing use and sophistication of AI in attacks is triggering an arms race between attackers and defenders. As attackers use AI in their attacks, defenders must rely on advanced AI-based detection and response solutions to develop and maintain effective defences. This results in a continuous cycle of innovation, where capabilities on both sides must evolve rapidly and systems on both sides must constantly adapt to each other's *learned* strategies. This can also place a heavy burden on attackers.[27]

Future trends in the use of AI in attacks

Despite the challenges described above, attackers will certainly continue to develop and use their AI-based capabilities in order to carry out their cyberattacks more effectively. The development of AI-based cyberattacks is expected to lead to the following worrying trends:

- *Fully autonomous cyberattack agents:* In the future, we can expect the emergence of fully autonomous AI-based attack systems that will be capable of independently planning a cyberattack, gather the necessary information, execute complex cyberattacks, and maintain a continuous presence, all without human intervention, based solely on an initial target or mission assigned to them. These autonomous cyberattack agents will have self-learning capabilities and will be able to adapt to defence systems.[28]

[25] Dilmegani 2026.
[26] Ragho–Chaudhari 2025; Prasad et al. 2025.
[27] Gil–Williams 2025; Erdész 2023.
[28] Moraes 2025; Schippers 2025.

- *The increasing use of AI-as-a-Service (AIaaS) for malicious purposes:* The availability of tools and services that can be used for AI-based cyberattacks will increase on the black market, enabling even less skilled or less technically knowledgeable attackers to launch highly sophisticated and effective AI-based attacks. This trend means that advanced attack techniques are no longer the preserve of nation states or large cybercriminal groups but are becoming more widely available. This phenomenon makes advanced attack capabilities possible and accessible to a wide range of cybercriminals, as it significantly lowers the threshold for entry into advanced cybercrime.[29]
- *Further refinement of social engineering attacks with the help of AI:* The use of generative AI, particularly deepfake audio and video technologies, already makes it possible to create extremely convincing and realistic content that can be used for social engineering attacks, and then to carry out effective attacks with the help of this content. On the one hand, this content will become even more authentic in the future, making it even more difficult to recognise that it is not real but produced with the help of AI, allowing attackers to imitate senior executives or trusted sources even more convincingly. On the other hand, in the future, it will be easier to produce such content with even less knowledge, even with the help of publicly available generative AI models, which will also lower the threshold for entry into advanced cybercrime.[30]
- *Adversary AI, or AI against AI:* Just as defence systems are increasingly using and developing AI-based defence capabilities to identify threats and manage incidents, responding to them as quickly as possible, the same is happening on the offensive side, i.e. attackers are also increasingly developing AI-based attack capabilities and will use AI-based techniques more widely when carrying out attacks. Thanks to these continuous developments on the attacker side, which include the creation and refinement of machine learning models against defence solutions, the adversary AI used in attacks is becoming increasingly sophisticated, for example, in the areas of evading defence AI systems and deliberately misleading defence algorithms.[31]
- *Cyber warfare with AI-based tools:* State-sponsored cyberattack groups are expected to devote significant human and financial resources in the near future to the development of AI-based cyber weapons and systems that will enable them to carry out large-scale, targeted, and covert attacks with much greater efficiency than is currently possible, even against targets with advanced defence systems including critical infrastructure. The rapid development and spread of AI attack capabilities will accelerate the pace of the changes outlined above, exacerbate threats, and lower the barrier to entry in this segment, which will jeopardise cybersecurity more than ever before. This development also means that future conflicts will shift even more to cyberspace, where AI-based offensive (and, on the other side, defensive) tools can provide a strategic advantage.[32]

[29] European Union Agency for Law Enforcement Cooperation 2025; Matejic–Wilson 2024.
[30] IProov 2023; Babaei et al. 2025.
[31] Gil–Williams 2025; CrowdStrike 2025.
[32] Anthropic 2025; Crichton et al. 2024.

Conclusion

This series of articles examined the malicious uses of artificial intelligence from the perspective of cyberattacks, building its content around the Cyber Kill Chain model. Based on the above, it can be concluded that artificial intelligence is not just the next step in technological development in cybersecurity, but a revolutionary event that brings fundamental changes in both its dynamics and quality. Its significance could perhaps be compared to the developmental leap of the first industrial revolution. The rapidly developing capabilities of AI in the areas of automation, adaptation, and complex pattern recognition enable attackers to carry out cyberattacks with unprecedented sophistication, using AI in every phase of the Cyber Kill Chain, i.e. the attack. From accelerating reconnaissance to generating advanced malware, through covert C2 communication, to effectively reaching attack objectives, AI can significantly increase the effectiveness, speed and covert nature of cyberattacks. On the one hand, by making advanced attack capabilities available to a wide range of people at low cost and with less and less knowledge required to use them, AI lowers the threshold for entry into cybercrime. On the other hand, it creates the possibility of fully autonomous cyberattack agents, fundamentally changing the cyber threat landscape.

Defenders must also be prepared to detect and counter AI-assisted attacks, and they must also use AI-based systems to develop effective defences. This phenomenon is resulting in a constantly escalating, spiral-like *AI arms race* between attackers and defenders, where AI-assisted capabilities are expected to develop exponentially on both sides, as is AI itself.

Those who work in incident management, i.e. cyber defence, are already encountering the fight against AI in the current landscape, but in the cybersecurity environment of the near future, this will increasingly become part of everyday life. In this new environment, defence systems will not only have to detect and respond to threats but also outsmart the AI models used by attackers.

In order to develop effective cyber defence, identify necessary areas for further development and recognise points for moving forward, it is advisable to conduct further studies and research. In this context, it is necessary to examine, on the one hand, what defence tools are currently used by cybersecurity experts in the various phases of CKC, which of these are already available today as AI-supported solutions, and what capabilities they currently have. On the other hand, it is also necessary to assess where and how artificial intelligence can help defenders in each phase of the CKC in the future. Following this, it is advisable to review AI-based defence trends and then compare the capabilities of the attacker and defender, demonstrating where and how effective response capabilities can be developed using artificial intelligence in response to attacker AI capabilities.

References

Abbadi, Driss – Lachkar, Abdelkader (2024): Cyber Threats in the Age of Artificial Intelligence: Exploiting Advanced Technologies and Strengthening Cybersecurity. *International Journal of Science and Research Archive,* 13(1), 2576–2588. Online: https://doi.org/10.30574/ijsra.2024.13.1.1961

Aboze, John B. (2025): A Comprehensive Guide to Data Exfiltration. *Lakera,* 21 May 2025. Online: www.lakera.ai/blog/data-exfiltration

Al-Azzawi, Mays – Doan, Dung – Sipola, Tuomo – Hautamäki, Jari – Kokkonen, Teri (2025): Red Teaming with Artificial Intelligence-Driven Cyberattacks: A Scoping Review. *ArXiv*. Online: https://doi.org/10.48550/arXiv.2503.19626

Anderson, Hyrum S. – Woodbridge, Jonathan – Filar, Bobby (2016): DeepDGA: Adversarially-Tuned Domain Generation and Detection. *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security,* 13–21. Online: https://doi.org/10.1145/2996758.2996767

Anthropic (2025): *Disrupting the First Reported AI-orchestrated Cyber Espionage Campaign.* Online: www.anthropic.com/news/disrupting-AI-espionage

Babaei, Reza – Cheng, Samuel – Duan, Rui – Zhao, Shangqing (2025): Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis. *Journal of Sensor and Actuator Networks,* 14(1). Online: https://doi.org/10.3390/jsan14010017

Boutin, Jean-Ian (2025): *ESET APT Activity Report Q2 2025 – Q3 2025.* Online: www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q2-2025-q3-2025/

Cherepanov, Anton – Strýček, Peter (2025): First *Known AI-powered Ransomware Uncovered by ESET Research.* Online: www.welivesecurity.com/en/ransomware/first-known-ai-powered-ransomware-uncovered-eset-research/

Crichton, Kyle et al. (2024): *Securing Critical Infrastructure in the Age of AI.* Center for Security and Emerging Technology. Online: https://doi.org/10.51593/20240032

CrowdStrike (2025): *CrowdStrike 2025 Global Threat Report.* Online: www.crowdstrike.com/en-us/resources/infographics/global-threat-report-2025/

Darktrace (2024): *Navigating a New Threat Landscape: Breaking Down the AI Kill Chain.* Online: www.darktrace.com/resources/navigating-a-new-threat-landscape

De Pasquale, Giulio – Grishchenko, Ilya – Iesari, Riccardo – Pizzaro, Gabriel – Cavallaro, Lorenzo – Kruegel, Christopher – Vigna, Giovanni (2024): *ChainReactor: Automated Privilege Escalation Chain Discovery via AI Planning.* Online: www.usenix.org/system/files/usenixsecurity24-de-pasquale.pdf

Dilmegani, Cem (2026): AI Data Quality in 2026: Challenges & Best Practices. *AIMultiple,* 27 March 2026. Online: https://research.aimultiple.com/data-quality-ai/

Erdész, Viktor (2023): *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben* [The Use of Artificial Intelligence in Military and National Security Intelligence]. Budapest: Katonai Nemzetbiztonsági Szolgálat.

European Union Agency for Law Enforcement Cooperation (2025): *IOCTA. Internet Organised Crime Threat Assessment 2025*. Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2813/4926508

Frisoni, Daniele (2020): *Potential Impact of Artificial Intelligence to C2 Systems.* Joint Air Power Competence Centre. Online: www.japcc.org/essays/potential-impact-of-artificial-intelligence-to-c2-systems/

Gil, Luis – Williams, Beth (2025): AI vs. AI: The Race Between Adversarial and Defensive Intelligence. *CrowdStrike,* 4 August 2025. Online: www.crowdstrike.com/en-us/blog/ai-vs-ai-cybersecurity-arms-race/

Holden, Alex (2023): Contending with Artificially Intelligent Ransomware. *ISACA,* 1 September 2023. Online: www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/contending-with-artificially-intelligent-ransomware

Humphries, Russ (2026): The Dark Side: How Threat Actors Are Using AI. *Connect Wise,* 3 March 2026. Online: www.connectwise.com/blog/the-dark-side-how-threat-actors-are-using-ai

IProov (2023): Understanding the Different Types of Generative AI Deepfake Attacks. *iProov,* 30 November 2023. Online: www.iproov.com/blog/generative-ai-attack-types-explained

ITszótár.hu (2025): Metamorf és polimorf kártevők: Ezen kártékony szoftverek működésének magyarázata [Metamorphic and Polymorphic Malware: An Explanation of How this Malicious Software Works]. *ITszótár.hu,* 15 May 2025. Online: https://itszotar.hu/metamorf-es-polimorf-kartevok-ezen-kartekony-szoftverek-mukodesenek-magyarazata/

Jain, Anu – Chhabra, Gurpal S. (2014). Anti-Forensics Techniques: An Analytical Review. *2014 Seventh International Conference on Contemporary Computing (IC3),* 412–418. Online: https://doi.org/10.1109/IC3.2014.6897209

Kewat, Rajnish (2025): What Are AI-Generated Rootkits and How Do They Threaten Enterprise Systems? *Cyber Security Training Institute,* 8 August 2025. Online: www.cybersecurityinstitute.in/blog/what-are-ai-generated-rootkits-and-how-do-they-threaten-enterprise-systems

Lee, Junho – Kwon, Jihoon – Seo, HyunA – Lee, Myeongyeol – Seo, Hyungyu – Jung, Jinho – Koo, Hyungjoon (2025): *BootKitty: A Stealthy Bootkit-Rootkit Against Modern Operating Systems.* Online: www.usenix.org/conference/woot25/presentation/lee

Lockheed Martin (s. a.): *Cyber Kill Chain.* Online: www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mailchimp (s. a.): *AI as a Service: The Latest Business Model.* Online: https://mailchimp.com/resources/ai-as-a-service/

Matejic, Nicole – Wilson, Chris (2024): Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service. *The Commonwealth Cyber Journal,* 2, 75–95.

Microsoft Security (2025): *What Is the Cyber Kill Chain?* Online: www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain

Moraes, Marco Túlio (2025): AI Agents: The New Frontier of Cybercrime Business Must Confront. *World Economic Forum,* 18 June 2025. Online: www.weforum.org/stories/2025/06/ai-agent-cybercrime-business/

Pappachan, Princy – Adi, Novi S. – Firmansyah, Gerry – Rahaman, Mosiur (2024): Deep Learning-Based Forensics and Anti-Forensics. In Abd El-Latif, Ahmed A. – Tawalbeh, Lo'ai – Mohanty, Manoranjan – Gupta, Brij B. – Psannis, Konstantinos E. (eds.): *Digital Forensics and Cyber Crime Investigation.* Boca Raton: CRC Press.

Powell, Evan (2025): Invisible C2 – Thanks to AI-powered Techniques. *Deep Tempo,* 14 March 2025. Online: https://medium.com/deeptempo/invisible-c2-thanks-to-ai-powered-techniques-462ef2624c8a

Prasad, Nilantha – Diro, Abebe – Warren, Matthew – Fernando, Mahesh (2025): A Survey of Cyber Threat Attribution: Challenges, Techniques, and Future Directions. *Computers & Security,* 157. Online: https://doi.org/10.1016/j.cose.2025.104606

Ragho, Soni R. – Chaudhari, Narendra (2025): Artificial Intelligence in Digital Forensics: A Review of Cyber-Attack Detection Models and Frameworks. *Journal of Information Systems Engineering and Management,* 10(57s). Online: https://jisem-journal.com/index.php/journal/article/view/12402

Raz, Md – Udeshi, Meet – Charan, Sai P. V. – Krishnamurthy, Prashanth – Khorrami, Farshad – Karri, Ramesh (2025): Ransomware 3.0: Self-Composing and LLM-Orchestrated. *Arxiv*. Online: https://doi.org/10.48550/arXiv.2508.20444

Sangfor Technologies (2025): AI DDoS: How Artificial Intelligence Is Changing the Face of Cyber Attacks. *Sangfor,* 9 September 2025. Online: www.sangfor.com/blog/cybersecurity/ai-ddos-attacks

Schippers, Raymond (2025): AI 2030: The Coming Era of Autonomous Cyber Crime. *Check Point,* 24 October 2025. Online: https://blog.checkpoint.com/executive-insights/ai-2030-the-coming-era-of-autonomous-cyber-crime/

Schröer, Saskia L. – Pajola, Luca – Castagnaro, Alberto – Apruzzese, Giovanni – Conti, Mauro (2025): Exploiting AI for Attacks: On the Interplay between Adversarial AI and Offensive AI. *ArXiv*. Online: https://arxiv.org/html/2506.12519

Tejedor, Jesús (2025): A Dangerous Alliance: The New Dark Web + AI Marketplace. *Telefónica,* 5 June 2025. Online: https://telefonicatech.com/en/blog/a-dangerous-alliance-how-ai-is-reshaping-the-dark-web-economy

Timilehin, Oladoja (2023): *Defending the Digital Horizon: Artificial Intelligence in Cybersecurity Warfare*.

Toulas, Bill (2025): LameHug Malware Uses AI LLM to Craft Windows Data-theft Commands in Real-time. *Bleeping Computer,* 17 July 2025. Online: www.bleepingcomputer.com/news/security/lamehug-malware-uses-ai-llm-to-craft-windows-data-theft-commands-in-real-time/

Trinckes, Jay (s. a.): AI Data Breach: Understanding their Impact and Protecting Your Data. *Thoropass*. Online: www.thoropass.com/blog/ai-data-breach

Utter, Jamison (2024): The Machine War Has Begun: Cybercriminals Leveraging AI in DDoS Attacks. *A10 Networks,* 24 September 2024. Online: www.a10networks.com/blog/the-machine-war-has-begun-cybercriminals-leveraging-ai-in-ddos-attacks/

Wang, Yulong – Sun, Tong – Li, Shenghong – Yuan, Xin – Ni, Wei – Hossain, Ekram – Poor, Vincent H. (2023): Adversarial Attacks and Defenses in Machine Learning-Empowered Communication Systems and Networks: A Contemporary Survey. *IEEE Communications Surveys & Tutorials*, 25(4), 2245–2298. Online: https://doi.org/10.1109/COMST.2023.3319492

Wang, Zhi – Liu, Chaoge – Cui, Xiang – Yin, Jie – Liu, Jiaxi – Wu, DI – Liu, Qixu (2022): DeepC2: AI-Powered Covert Command and Control on OSNs. In Alcaraz, Cristina – Chen, Liqun – Li, Shujun – Samarati, Pierangela (eds.): *Information and Communications Security.* Cham: Springer, 394–414. Online: https://doi.org/10.1007/978-3-031-15777-6_22

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 1. szám 41–55.
DOI: 10.32567/hm.2026.1.3

István Paráda[1]

Cyber Disruptions in Aviation Infrastructure

The CrowdStrike Outage

Abstract

This paper examines the intersection between civilian aviation cyber incidents and military logistics resilience, focusing on the systemic implications of the 2024 CrowdStrike global outage. Between 2018 and 2025, a series of airport IT and cybersecurity failures – ranging from ransomware to defence software malfunctions – exposed the vulnerabilities of dual-use infrastructures that serve both civil and military air mobility. The 2024 CrowdStrike event, which disrupted millions of systems worldwide, revealed the operational fragility of shared digital dependencies in air logistics networks. Drawing on data from FAA, ICAO and ENISA, this analysis identifies key lessons for defence logistics planners and cybersecurity policymakers seeking to enhance resilience against cascading failures.

Keywords: aviation cybersecurity, CrowdStrike incident, ENISA, NATO

Introduction: Cyber dependence and dual-use aviation logistics

Modern military logistics relies heavily on civilian aviation networks and digital infrastructure. Shared systems such as Jeppesen's MilPlanner and multinational airport IT environments blur the boundaries between civil and defence operations. This convergence enhances interoperability and efficiency, yet simultaneously creates tightly coupled digital dependencies that may amplify systemic vulnerability. Events such as the CrowdStrike 2024 outage highlight how a single commercial software update can propagate through defence logistics systems, affecting readiness, supply chain coordination and strategic mobility. Unlike conventional cyberattacks, this event originated from a non-malicious configuration failure, yet its operational effects resembled those of a coordinated systemic attack.

[1] CIS Operations Officer, NATO Support and Procurement Agency, e-mail: paradaistvan@gmail.com

This study examines aviation-related cyber and IT disruptions between 2018 and 2025 through a dual-use resilience lens. It addresses two research questions:

RQ1: What lessons does the CrowdStrike outage reveal about cybersecurity challenges in aviation and military operations?

RQ2: How have aviation and military organisations adapted to increasing cybersecurity dependency?

Literature review and methodology

The study adopts a qualitative, document-based analytical methodology. Empirical inputs are derived exclusively from publicly available institutional reports, incident reviews and regulatory publications issued by organisations such as ENISA,[2] FAA,[3] ICAO,[4] NATO CCDCOE[5] and NIST[6] between 2018 and 2025. Quantitative figures cited in the analysis are reproduced from these sources and are used illustratively rather than as independently generated datasets. Analytical inferences are explicitly distinguished from empirical observations. Documented incident characteristics – such as outage duration, affected systems and geographic scope – form the empirical baseline, while interpretations concerning cascading effects, logistics implications, and doctrinal relevance are derived through comparative analysis informed by resilience theory. Normative conclusions are presented as analytical implications rather than empirically verified causal claims.

A total of eleven significant aviation-related cyber and IT incidents were analysed, spanning the 2018–2025 period. Incident selection followed predefined inclusion criteria to enhance procedural transparency. Cases were incorporated into the dataset if they involved documented operational disruption affecting aviation IT or digital service infrastructure, were supported by official institutional reporting or credible post-incident documentation, included verifiable information regarding recovery duration, and demonstrated potential relevance for dual-use civilian–military aviation systems. Incidents lacking reliable documentation on operational scope or recovery timeframe were excluded from the comparative assessment.

Data collection was conducted through structured keyword searches in institutional databases and official publications using terms such as “aviation IT outage”, “airport ransomware”, “flight planning system failure” and “cybersecurity software update disruption”. Primary reliance was placed on institutional documentation issued by regulatory authorities and aviation agencies. Journalistic sources were used solely for contextual clarification and were not treated as primary evidentiary material.

Each incident was coded across three analytical dimensions forming the tri-axial model. The first dimension, Cyber Layer, categorises the documented technical origin of disruption, distinguishing among conventional software failures, malicious cyberattacks,

[2] European Union Agency for Cybersecurity.
[3] Federal Aviation Administration.
[4] International Civil Aviation Organization.
[5] NATO Cooperative Cyber Defence Centre of Excellence.
[6] National Institute of Standards and Technology.

security software malfunctions and cyber defence system malfunctions. Classification was based strictly on reported technical cause rather than inferred intent. The second dimension, Operational Reach, captures the geographic and organisational scope of impact and was assessed according to documented spread across local, sectoral, or global aviation systems. The third dimension, Recovery Time, reflects the duration required to restore operational functionality and was coded using consistent temporal thresholds based on documented restoration timelines.

Operationalisation of these variables followed uniform category definitions to ensure internal coherence across cases. Analytical interpretations are explicitly separated from empirical observations; documented incident characteristics constitute the evidentiary foundation, while resilience-related inferences are derived through structured comparison.

This study makes three distinct scholarly contributions to the fields of aviation cybersecurity and military logistics resilience. First, it conceptualises aviation-sector cyber and IT disruptions as dual-use systemic dependencies, demonstrating how failures originating in civilian commercial cybersecurity products can propagate into military logistics, mission planning and strategic air mobility systems. While prior studies have examined cyber threats or aviation disruptions separately, this paper analytically integrates these domains through a logistics-resilience perspective. Second, the study introduces a tri-axial analytical model, Cyber Layer – Operational Reach – Recovery Time, that enables structured comparison of heterogeneous cyber incidents across civilian and military aviation contexts. This model extends existing critical infrastructure resilience frameworks by explicitly linking technical failure modes (including non-malicious software errors) to operational and mission-level degradation. Third, through the case study of the 2024 CrowdStrike outage, the paper reframes endpoint cybersecurity software from a protective IT function into an operational dependency with doctrinal implications. The analysis demonstrates that cybersecurity mechanisms themselves can become systemic risk multipliers when deployed at scale without coordinated validation and resilience planning.

Cybersecurity challenges in civil and military airlift: A review of existing approaches and analytical gaps

The aviation sector has long been recognised as a critical infrastructure with increasing exposure to cyber risks due to its reliance on interconnected information and communication technologies. Existing literature and institutional analyses emphasise that aviation cybersecurity challenges extend beyond isolated technical vulnerabilities and involve systemic dependencies across airports, airlines, air navigation service providers, and supporting digital services.[7] Regulatory studies by ICAO, EASA[8] and ENISA primarily focus on threat identification, risk categorisation and compliance-based security management. While these works provide a comprehensive overview of threat

[7] Ukwandu et al. 2022; ENISA 2023.
[8] European Union Aviation Safety Agency.

landscapes and regulatory responses, they largely adopt a threat-centric perspective. Less attention is given to non-malicious failures originating from software updates, configuration errors, or internal system dependencies, despite their demonstrated operational impact on aviation continuity. A parallel body of literature addresses cyber resilience in complex socio-technical systems, emphasising concepts such as cascading failures, tight coupling and systemic vulnerability.[9] Resilience theory suggests that highly integrated systems may amplify disturbances, allowing localised technical failures to propagate across organisational and geographic boundaries. Studies on critical information infrastructure protection further argue that protective mechanisms themselves can become sources of disruption when improperly validated or centrally deployed.[10] These studies typically remain sector-agnostic or focus on energy, telecommunications, or industrial systems. Aviation-specific applications of cascading failure theory remain limited, and explicit links to military air mobility and logistics operations are rarely developed.

Military logistics literature increasingly recognises cyberspace as a critical enabler of operational readiness and strategic mobility. NATO doctrine and defence-focused analyses emphasise the shift from information assurance toward mission assurance, reflecting the understanding that digital systems underpin planning, coordination, and execution across domains.[11] Studies on defence supply chains highlight the growing dependence on civilian infrastructure and commercial software providers, particularly in airlift and transport operations. Despite this recognition, much of the military-focused literature treats cyber risk primarily as an external threat or intelligence problem. Civilian aviation systems and commercial cybersecurity products are often assumed to be reliable enablers rather than potential sources of systemic disruption. As a result, the operational implications of shared digital dependencies between civilian aviation and military logistics remain under-theorised, especially in the context of non-hostile cyber disruptions.

Taken together, existing literature provides substantial insight into aviation cybersecurity threats, resilience theory and military logistics assurance. However, these bodies of work largely remain analytically siloed. Aviation cybersecurity studies rarely extend their analysis into military logistics implications, while defence logistics literature seldom incorporates civilian cybersecurity failures as systemic risk factors. The present study addresses this gap by integrating these strands through a dual-use logistics resilience perspective. By analysing aviation cyber incidents – including non-malicious failures – across a multi-year dataset and applying a tri-axial analytical model, the study moves beyond narrative case description toward structured comparison. In doing so, it positions cybersecurity software and digital service dependencies as operational variables rather than purely technical considerations.

[9] Nowakowski et al. 2015; Johnson 2013: 61–92.
[10] McCreight 2019.
[11] Bhargava 2024; Haig–Kovács 2012.

Airport IT and cybersecurity disruptions (2018–2025): Patterns of systemic failure

The resilience of critical aviation infrastructure is challenged by a heterogeneous set of risk vectors. Traditional scholarship categorises these into external physical threats – such as natural disasters, power grid blackouts and kinetic terrorist acts – and internal technical vulnerabilities. However, the increasing digitisation of dual-use logistics has shifted the primary risk profile toward ICT[12] infrastructure dependencies. Recent studies emphasise that the most frequent causes of IT outages in complex operating systems are not necessarily external attacks, but rather Software Errors and Software Aging.[13] Software aging – the cumulative degradation of system performance due to resource exhaustion and error buildup – significantly increases the probability of catastrophic failure in systems that require high availability, such as ATM[14] and military C2[15] networks.[16]

The transition from a technical failure to a mission-level disruption is driven by downtime.

In the context of aviation:

- Breadth of impact: Because operating system outages affect all dependent applications, a kernel-level failure (like the CrowdStrike BSOD[17]) effectively decapitates the entire operational stack.
- Economic consequences: Unanticipated outages in major aviation hubs result in considerable loss of economic activity. For dual-use infrastructures, this translates into a loss of Mission Assurance, where the inability to process flight plans or ground handling data halts the movement of strategic assets.

Between 2018 and 2025, eleven major aviation-related cyber incidents were identified and analysed (Table 1). The incidents span a range of geographic locations, threat vectors and technical origins, including conventional software failures, ransomware attacks, security software malfunctions, and defence-related cyber system errors. While several incidents originated in localised operational contexts, others produced sector-wide or global effects, underscoring the increasing interconnectedness of aviation digital infrastructure. The dataset confirms that aviation operates as a tightly coupled "system of systems", where failures at the IT or cybersecurity layer can propagate rapidly into operational disruption. Importantly, the dataset includes both malicious incidents (e.g. ransomware attacks) and non-malicious failures (e.g. faulty software updates), allowing comparative assessment of their respective operational impacts. This distinction is central to the analytical framework applied in this study.

[12] Information and Communication Technologies.
[13] Bovenzi et al. 2013.
[14] Air Traffic Management.
[15] Command-and-Control.
[16] Dos Santos – Matias 2017; Dos Santos et al. 2018; Noë et al. 2021.
[17] Blue screen of death: It is used to indicate a system crash, in which the operating system reaches a critical condition where it can no longer operate safely.

As shown in Figure 1, data-related threats and ransomware dominate the aviation cyber threat landscape, accounting together for over two-thirds of reported incidents. An examination of cybersecurity issues in the aviation sector in 2022 revealed that 71% of cybercriminals aimed to obtain login credentials to infiltrate IT systems. Out of those attacks, 25% were DDoS[18] incidents, while 4% of cybercriminals intended to compromise file integrity.[19] The transportation industry has witnessed an increase in cybersecurity incidents in the last seven years. Aviation, referred to as a "system of systems", consists of numerous technologies, individuals and procedures, making the supply chain vulnerable to risks. In 2025, a series of assaults targeted major U.S. and EU airlines in the aviation sector. The escalation of cyber threats against aviation infrastructure is a documented trend, with institutional reports indicating a consistent increase in incident frequency since 2019. Nevertheless, security experts cautioned that the issue will only become more severe. The operational stress placed on legacy aviation IT infrastructure has exposed latent vulnerabilities in high-demand environments. "Even in the absence of a cyberattack, antiquated technologies and vulnerable logistics can result in significant disruptions", said Jiwon Ma, senior policy analyst at FDD's[20] Center on Cyber and Policy Innovation.[21]

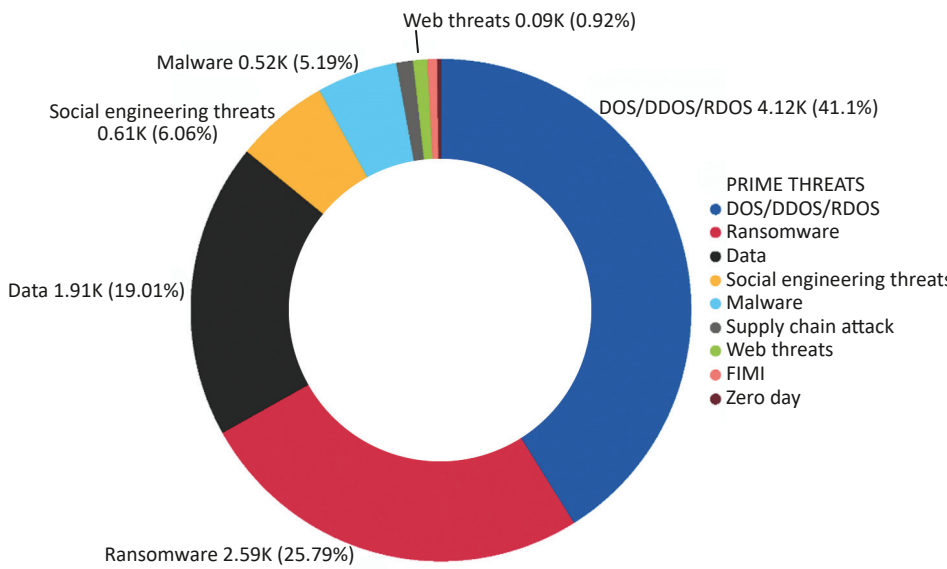


Figure 1: Distribution of incident by threats types (2023–2024)
Source: ENISA 2024

[18] Distributed Denial-of-Service attack is a cyberattack that overwhelms a targeted server, website, or network with a flood of malicious internet traffic from multiple compromised systems (a botnet) to disrupt normal service, making it unavailable for legitimate users.
[19] Thales 2025.
[20] Foundation for Defense of Democracies (FDD) publishes research on foreign policy and security issues, focusing on subjects such as nuclear non-proliferation, cyber threats, sanctions, illicit finance.
[21] Traynor 2025.

To illustrate the operational relevance of aviation cybersecurity disruptions, it is useful to examine a selection of documented incidents from recent years. Table 1 summarises major cyber and IT-related events affecting airports, air navigation services, and aviation-supporting digital infrastructure between 2018 and 2025. The selected cases demonstrate varying combinations of technical origin, operational reach and recovery duration, and several exhibit direct relevance for global aviation continuity and military air-mobility operations.

Table 1: Documented airport and aviation cyber incidents (2018–2025)

Year	Location	Incident description	Cyber layer	Recovery time	Operational reach
2018	Bristol (U.K.)	Ransomware attack	Cyberattack[22]	Prolonged	Sectoral
2019	Atlanta (USA)	CBP system failure	Software Failure[23]	Short	Local
2019	Heathrow & Gatwick (U.K.)	Windows update crash	Software Failure[24]	Short	Sectoral
2020	San Francisco (SFO)	Maze ransomware	Cyberattack[25]	Prolonged	Sectoral
2021	Global (Microsoft/Akamai)	Defender update (BSOD)	Security software error[26]	Medium	Global
2022	Jeppesen/Mil-Planner	Ransomware attack	Cyberattack[27]	Prolonged	Global
2023	FAA (USA)	Database corruption (NOTAM[28] failure)	Software failure[29]	Medium	Sectoral
2024	NATS (U.K.)	Flight parser failure	Software failure[30]	Medium	Sectoral
2024	Copenhagen (Denmark)	ESET update disruption	Security software error[31]	Medium	Sectoral
2024	Global (CrowdStrike Falcon)	Kernel driver crash (BSOD)	Cyber defence software error[32]	Prolonged	Sectoral
2025	Frankfurt (Germany)	Ransomware attack	Cyberattack[33]	Prolonged	Global

Source: compiled by the author

[22] Zanni 2018.
[23] Rockwell 2019.
[24] Jolly 2019.
[25] Cyble 2020.
[26] Sundaram 2021.
[27] Hunorfi et al. 2024: 101–120.
[28] Notice to Airmen is a notice containing information concerning the establishment, condition or change in any aeronautical facility, service, procedure or hazard, the timely knowledge of which is essential to personnel concerned with flight operations.
[29] Nolen 2023.
[30] Halliwell et al. 2024.
[31] Barrett 2024.
[32] CrowdStrike 2024.
[33] Paganini 2025.

A tri-axial model for assessing aviation cyber disruptions

To move beyond descriptive incident reporting, each disruption was analysed using the proposed tri-axial model, which links three analytical dimensions: cyber layer, operational reach, recovery time.

Cyber layer categorises the technical origin of the disruption as: software failure, cyberattack, security software malfunction, or cyber defence system malfunction. Operational reach captures the spatial and organisational scope of impact, classified as local, sectoral, or global. Recovery time reflects the duration required to restore operational functionality, categorised as short-term (hours), medium-term (days), or prolonged (weeks or longer).

Applying this model reveals clear structural patterns. Conventional software failures – such as the 2019 CBP[34] system outage in Atlanta – tended to remain locally contained and were resolved within short recovery periods. By contrast, ransomware incidents exhibited broader operational reach and longer recovery times due to system restoration requirements and forensic processes. Most notably, incidents originating in the security and defence software layer consistently demonstrated the widest operational reach. The 2022 Jeppesen/MilPlanner disruption and the 2024 CrowdStrike Falcon outage both propagated across national and alliance-level aviation systems, despite differing in intent and technical trigger. This finding indicates that centralised cybersecurity tools represent a distinct category of systemic risk within aviation and military logistics ecosystems.

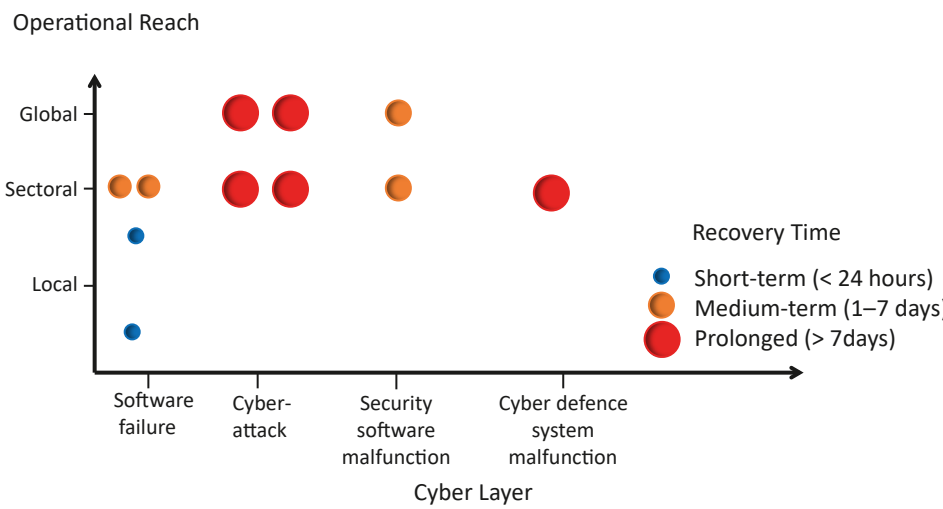


Figure 2: Tri-axial model for assessing aviation cyber disruptions

Source: compiled by the author based on incident data collected from ENISA, FAA, ICAO, and publicly available post-incident reports (2018–2025)

[34] Customs and Border Protection: Protecting the American people, safeguarding our borders and enhancing the nation's economic prosperity.

Figure 2 visualises three analytical dimensions: cyber layer (x-axis), operational reach (y-axis) and recovery time (encoded by marker size). Recovery time categories are defined as short-term (< 24 hours), medium-term (1–7 days) and prolonged (> 7 days). The cyber layer axis is ordered according to increasing systemic coupling, from conventional software failures to centrally deployed cyber defence systems. The model illustrates those incidents originating in higher-order cyber layers that tend to combine wider operational reach with longer recovery periods, even in the absence of malicious intent. When mapped across the tri-axial dimensions, the incidents cluster into three analytically relevant patterns. First, localised software failures are frequent but operationally manageable. Although such failures can cause immediate delays and economic losses, their limited propagation potential and relatively rapid recovery reduce their strategic significance. Second, malicious cyberattacks, particularly ransomware, produce asymmetric operational effects. While not always global in reach, these incidents often result in prolonged recovery times and secondary impacts such as data exfiltration, regulatory exposure and reputational damage. Their relevance to military logistics lies primarily in contingency planning and redundancy rather than systemic interdependence. Third, and most critical, non-malicious failures in cybersecurity and defence software exhibit high-impact, low-frequency characteristics. These events combine global operational reach with prolonged recovery potential, despite originating from trusted and widely deployed systems. The model demonstrates that such failures bypass traditional threat-centric risk models, as their effects stem from architectural centralisation and automated propagation mechanisms rather than adversarial action. This pattern supports resilience theory arguments that tightly coupled systems are vulnerable to cascading "safe-mode" failures, where protective mechanisms inadvertently trigger operational paralysis.

The CrowdStrike 2024 outage was selected for in-depth case analysis due to its global reach, non-malicious origin, and direct relevance to both civilian aviation and military logistics systems. The case serves as an analytical stress test for the proposed model rather than as a representative incident.

Case study: The 2024 CrowdStrike outage as a systemic cyber failure

The CrowdStrike Falcon, recognised as a NGAV[35] cybersecurity platform, can aid different sectors. In contrast to traditional antivirus solutions that mainly depend on signature-based detection (recognising known malware by matching files with a signature database), NGAV utilises sophisticated technologies to deliver broader and more proactive security. Conventional antivirus systems have transformed into contemporary versions like Endpoint Detection & Response.[36] Through monitoring the actions of a programme (e.g. trying to reach sensitive files or execute unauthorised modifications), NGAV can detect possible threats by analysing behaviour patterns instead of depending only on recognised malware signatures. NGAV systems utilise

[35] Next Generation Antivirus.
[36] Basit Ajmal et al. 2022.

machine learning algorithms to identify patterns and irregularities in data. These algorithms draw from past and evolving threats, enhancing their capacity to detect new and unfamiliar malware. AI-powered NGAV can foresee and thwart attacks by examining extensive datasets and identifying possible vulnerabilities or attack vectors prior to their exploitation. NGAV typically incorporates EDR[37] features, enabling the identification, examination and reaction to security incidents on endpoints. EDR tools offer comprehensive insight into endpoint actions and allow quick reactions to possible threats. EDR capabilities assist in grasping the characteristics of an attack, its propagation, and the measures implemented, thereby helping to reduce future risks and enhance security posture.[38]

The 2024 CrowdStrike incident represents a high-impact systemic failure within globally distributed digital supply chains. Triggered by a faulty Falcon sensor update, the event caused over 8.5 million Windows-based systems to crash globally within hours.[39] The technical failure resulted in an immediate 11% reduction in the company's market capitalisation.[40] The effects of the global tech outage on Friday, 19 July 2024, persisted into Saturday, with employees from airlines, banks, hospitals, and other vital sectors focused on remediating operational backlogs resulting from the systemic disruption of Windows-based endpoint devices.[41] Numerous industries were affected by the tech failure, but none contain the public data found in the aviation industry. The kernel driver update, intended to enhance EDR capabilities, contained an invalid memory reference that caused immediate system crashes (BSOD) upon boot. The incident disrupted airline check-in systems, ground operations, logistics, and Service Desk platforms across major airports including Heathrow, Frankfurt, Sydney and Atlanta. Among those affected were Jeppesen's flight planning systems – integral to various military transport operations. This demonstrated the critical interdependence between civilian cybersecurity software vendors and defence operational continuity. According to ENISA's 2024 review, the outage temporarily degraded situational awareness in several European transport command centres. While the incident was not the result of a cyberattack, its systemic effects mirrored those of a coordinated disruption, revealing that resilience gaps persist even in peacetime. This reinforces the argument that digital supply chain assurance must become a core pillar of NATO's logistics doctrine.

Within the dataset, the 2024 CrowdStrike outage represents an extreme but analytically revealing case. Classified under the tri-axial model as a cyber defence system malfunction with global operational reach and medium-to-prolonged recovery time, the incident illustrates how endpoint security software has become embedded in the operational fabric of aviation and military logistics. Unlike ransomware incidents, the CrowdStrike disruption did not involve data compromise or hostile intent. Nevertheless, its effects were comparable to a coordinated cyberattack, disrupting airline check-in systems, ground operations, Service Desk platforms, and flight-planning tools used in

[37] Endpoint Detection and Response.
[38] Pinheiro et al. 2019.
[39] Weston 2024.
[40] Coulter 2024.
[41] Rosman 2024.

both civilian and military contexts. The incident thus demonstrates that cybersecurity assurance failures can degrade mission assurance even in the absence of adversarial activity. From an analytical perspective, the CrowdStrike case validates the model's central claim: the cyber layer in which a failure originates is a stronger predictor of operational reach than the maliciousness of the event. This insight distinguishes the present analysis from narrative incident reporting and underscores the model's decision-support value for defence logistics planners.

Across the dataset, the tri-axial model enables systematic comparison of heterogeneous incidents and highlights a previously under-theorised risk category: centrally deployed defensive cyber dependencies. While aviation cybersecurity discourse often prioritises external threats, the results suggest that internal technological dependencies pose equal or greater risk to operational continuity. The analysis therefore reframes aviation cybersecurity from a threat-centric paradigm toward a dependency-centric resilience problem. For military air mobility, this implies that logistics resilience can no longer be assured solely through network hardening or threat detection. Instead, resilience must account for update governance, cross-domain testing, rollback capability, and the operational role of Service Desks as crisis management nodes.

The 2024 CrowdStrike incident serves as a pivotal reminder that cybersecurity tools themselves can be potential vectors of disruption. Future strategies should include rigorous sandbox testing, redundant Service Desk failover procedures, and internationally standardised incident response protocols aligned with ICAO Annex 19 and ISO/IEC 27035. Three strategic insights emerge from this assessment. First, civilian infrastructure and military logistics share a growing digital dependency that erodes traditional redundancy. Second, commercial cybersecurity products – though essential – introduce systemic risks when deployed without coordinated validation protocols across the systems. Third, information-sharing and pre-emptive sandbox testing between civilian IT vendors and defence agencies should be institutionalised under NATO and EU frameworks.

These findings align with RAND's (2023) and NIST's (2025) emphasis on cross-domain resilience: the ability of logistics networks to absorb and recover from disruptions regardless of origin. They also support ICAO's emerging guidance on dual-use cyber risk management within aviation ecosystems.[42]

Conclusions

Rather than treating the 2024 CrowdStrike outage as an isolated technical failure, this study interprets it as a systemic stress test of dual-use aviation logistics. The findings demonstrate that cybersecurity assurance has become inseparable from operational and mission assurance in both civilian and military airlift ecosystems. This section draws on the case study material discussed above to address the research questions set out in the introduction section.

[42] Lucas et al. 2024.

RQ1 inquired about the lessons the CrowdStrike outage reveals about cybersecurity challenges in aviation and military operations. The analysis demonstrates that cyber risk in aviation logistics is increasingly systemic rather than threat-driven. The 2024 CrowdStrike incident shows that non-malicious failures in widely deployed cybersecurity software can produce effects comparable to deliberate cyberattacks, disrupting mission planning, Service Desk operations, and logistics coordination across civilian and military domains. The key lesson is that digital protection mechanisms have become operational dependencies. As a result, resilience planning must extend beyond perimeter defence and threat detection to include update validation, rollback capability and cross-domain impact assessment. The lessons drawn from the CrowdStrike and earlier MilPlanner[43] outages reveal that cyber risk in aviation logistics is systemic, not incidental. Both events exposed a fundamental fragility in global air mobility: the lack of cross-domain testing, centralised update validation, and real-time incident coordination between civil and defence operators.

RQ2 examined how aviation and military organisations adapted to increasing cybersecurity dependency. The findings indicate a gradual but incomplete shift from information assurance toward mission assurance. While aviation and defence organisations increasingly recognise cyberspace as an operational domain, governance structures and validation practices remain fragmented. The CrowdStrike case illustrates that current adaptation efforts focus primarily on external threats, leaving internal technological dependencies insufficiently managed. Effective adaptation therefore requires integrating cybersecurity assurance into logistics doctrine, redefining the role of IT Service Desks as operational nodes, and institutionalising civil–military coordination mechanisms at alliance level.

At a strategic level, the CrowdStrike outage also redefined how alliances like NATO and the EU perceive logistics resilience. It exposed that cyber vulnerabilities are not confined to attacks but may emerge from trusted internal systems. This challenges the conventional dichotomy between threat defence and operational continuity. Future frameworks must integrate cybersecurity assurance into logistics doctrine, emphasising layered validation, redundant infrastructure and shared situational intelligence. Regular joint cyber exercises between civilian aviation partners, software providers, and defence logistics units could transform reactive recovery into proactive deterrence.

In conclusion, the 2024 CrowdStrike incident serves as a critical empirical case requiring the integration of digital supply chain resilience into logistics doctrines. It showed that worldwide military and civilian movement relies on a delicate network of digital dependencies that go beyond jurisdictional and organisational limits. The future of logistics resilience will depend on how quickly institutions adapt to this new reality: where cybersecurity, service continuity and strategic logistics are inseparable. The path forward demands a paradigm shift – from technology-centric security to mission-centric cyber governance – ensuring that the next global disruption becomes an opportunity for foresight rather than a failure of preparation.

[43] Paráda–Tóth 2024: 167–182.

References

Barrett, Michael (2024): How has the Global IT Outage Affected Denmark? *The Local,* 19 July 2024. Online: www.thelocal.dk/20240719/how-is-global-it-outage-affecting-denmark#:~:text=Danish%20rail%20operator%20DSB's%20website%20is%20down,as%20the%20effects%20of%20the%20outage%20rippled

Basit Ajmal, Abdul – Khan, Shawal – Jabeen, Farhana (2022): Defeating Modern Day Anti-Viruses for Defense Evaluation. *2022 International Conference on Frontiers of Information Technology,* 255–260. Online: https://doi.org/10.1109/FIT57066.2022.00054

Bhargava, Amit Kumar (2024): Cybersecurity in Aerospace: A Military Perspective. *Blue Yonder,* 1(1). Online: https://journals.capsindia.org/index.php/byj/article/view/48/47

Bovenzi, Antonio – Lopez, Javier Alonso – Yamada, Hiroshi – Russo, Stefano – Trivedi, Kishor S. (2013): Towards Fast OS Rejuvenation: An Experimental Evaluation of Fast OS Reboot Techniques. *2013 IEEE 24th International Symposium on Software Reliability Engineering,* 61–70. Online: https://doi.org/10.1109/ISSRE.2013.6698905

Coulter, Martin (2024): CrowdStrike Chaos Could Prompt Rethink among Investors, Customers. *Reuters,* 20 July 2024. Online: www.reuters.com/technology/cybersecurity/crowdstrike-chaos-could-prompt-rethink-among-investors-customers-2024-07-19/

CrowdStrike (2024): Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD). *CrowdStrike,* 24 July 2024. Online: www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

Cyble (2020): SFO Struck by a Web Compromise. *Cyber News,* 13 April 2020. Online: https://cyble.com/blog/sfo-struck-by-a-web-compromise/

Dos Santos, Caio A. R. – Matias, Rivalino Jr. (2017): An Empirical Study on Patterns of Failure Causes in a Mass-market Operating System. *Proceedings of the ACM Symposium on Applied Computing,* 1542–1547. Online: https://doi.org/10.1145/3019612.3019740

Dos Santos, Caio A. R. – Prince, Marcela A. – Matias, Rivalino Jr. – Fonseca Maciel, Vinicius (2018): Reliability Assessment of Commercial Off-the-shelf Operating System Software: An Empirical Study. *Brazilian Symposium on Computing Systems Engineering,* 201–206. Online: https://doi.org/10.1109/SBESC.2018.00038

ENISA (2023): *ENISA Threat Landscape 2021–2022.* Online: https://doi.org/10.2824/553997

ENISA (2024): *ENISA Threat Landscape 2024.* Online: https://doi.org/10.2824/0710888

Federal Aviation Administration (FAA) (2024): *After Action Report on January 2023 Notice to Air Missions Database Failure.* Online: www.governmentattic.org/55docs/FAAaarJan2023NTAMdbfail2023.pdf

Haig, Zsolt – Kovács, László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* [Critical Infrastructures and Critical Information Infrastructures]. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/kovasz-tanulmany.pdf

Halliwell, Jeff – Chambers, Sarah – Cropper, Phil – Foulsham, Mark (2024): *Independent Review of NATS (En Route) Plc's Flight Planning System Failure on 28 August 2023.* Online: www.caa.co.uk/publication/download/23337

Hunorfi, Péter – Paráda, István – Farkas, Tibor (2024): Kiberbiztonsági kihívások a légi közlekedésben – Kronológiai folyamat a Boeing elleni kibertámadások tükrében [Cybersecurity Issues in Aviation – Timeline of Cyber Crimes against Boeing]. *Hadmérnök,* 19(1), 101–120. Online: https://doi.org/10.32567/hm.2024.1.6

ICAO (2025): *Doc 10213 — Unrestricted. Global Cyber Risk Considerations.* Online: www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Doc-10213-Unedited-Global-Cyber-Risk-Considerations.EN_.pdf

Johnson, Chris W. (2013): Lessons from Major Incidents Influencing and Influenced by Telecoms Failures. In Théron, Paul – Bologna, Sandro (eds.): *Critical Information Infrastructure Protection and Resilience in the ICT Sector.* Hershey: IGI Global, 61–92. Online: https://doi.org/10.4018/978-1-4666-2964-6.ch004

Jolly, Jasper (2019): Passenger Anger as Tens of Thousands Hit by BA Systems Failure. *The Guardian,* 7 August 2019. Online: www.theguardian.com/business/2019/aug/07/british-airways-it-glitch-causes-disruption-for-passengers-delays

Lucas, Rebecca – Ekström, Thomas – Fusaro, Paola – Hastings Roer, Elizabeth – Retter, Lucia (2024): *Toward Defense Supply Chain Disruption Management. A Research Agenda for Defense Supply Chain Resilience*. RAND Research Report. Online: www.rand.org/content/dam/rand/pubs/research_reports/RRA2500/RRA2504-1/RAND_RRA2504-1.pdf

McCreight, Robert (2019): Grid Collapse Security, Stability and Vulnerability Issues: Impactful Issues Affecting Nuclear Power Plants, Chemical Plants and Natural Gas Supply Systems. *Journal of Homeland Security and Emergency Management,* 16(1). Online: https://doi.org/10.1515/jhsem-2018-0021

Noë, Nyala – Tuzovic, Emina – McArthur, Frederik S. – Thompson Carroll, Angus (2021): Improving Loss Prevention in High Hazard Industries Through the Evaluation of Safety Culture and Error Traps from Structured and Unstructured Data Using Machine Learning. *Institution of Chemical Engineers Symposium Series,* (168). Online: www.icheme.org/media/27736/hazards-31-paper-40-noe.pdf

Nolen, Billy (2023): *The Federal Aviation Administration's NOTAM System Failure and its Impacts on a Resilient National Airspace.* Statement of Billy Nolen, Acting Administrator Federal Aviation Administration Hearing before the United States Senate Committee on Commerce, Science, and Transportation Notice to Air Missions System, February 15, 2023. Online: www.transportation.gov/federal-aviation-administrations-notam-system-failure-and-its-impacts-resilient-national-airspace

Nowakowski, Tomasz – Młyńczak, Marek – Jodejko-Pietruczuk, Anna – Werbińska-Wojciechowska, Sylwia eds. (2015): *Safety and Reliability. Methodology and Applications.* Boca Raton: CRC Press. Online: https://doi.org/10.1201/b17399

Paganini, Pierluigi (2025): Safepay Ransomware Group Claims the Hack of Professional Video Surveillance Provider Xortec. *Security Affairs,* 26 October 2025. Online: https://securityaffairs.com/183868/malware/safepay-ransomware-group-claims-the-hack-of-professional-video-surveillance-provider-xortec.html

Paráda, István – Tóth, András (2024): A NATO katonai légi szállítási képességek kibervédelmi aspektusai [Cybersecurity Challenges for NATO Military Air Transport Operations]. *Hadmérnök,* 19(4), 167–182. Online: https://doi.org/10.32567/hm.2024.4.12

Pinheiro, Ricardo – Lima, Sidney – Fernandes, Sergio – Silva, Sthéfano H. M. T. (2019): Next Generation Antivirus Applied to Jar Malware Detection Based on Runtime Behaviors Using Neural Networks. *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design,* 28–32. Online: https://doi.org/10.1109/CSCWD.2019.8791864

Rockwell, Mark (2019): Software Bug Caused CBP Airport System Outage. *FCW,* 19 August 2019. Online: www.nextgov.com/modernization/2019/08/software-bug-caused-cbp-airport-system-outage/210982/

Rosman, Rebecca (2024): Disruptions Continue after an IT Outage Affects Millions around the Globe. *NPR,* 20 July 2024. Online: www.npr.org/2024/07/20/g-s1-12487/crowdstrike-microsoft-outage-update

Sundaram, Mani (2021): Akamai Summarizes Service Disruption. *Akamai,* 22 July 2021. Online: www.akamai.com/blog/news/akamai-summarizes-service-disruption-resolved

Thales (2025): *Aviation Sector Sees 600% Year-on-year Increase in Cyberattacks.* Online: www.thalesgroup.com/en/news-centre/press-releases/aviation-sector-sees-600-year-year-increase-cyberattacks

Traynor, Orlaith (2025): *The Global Impact of Aviation Cyberattacks.* Online: https://cybelangel.com/blog/the-global-impact-of-aviation-cyberattacks/

Ukwandu, Elochukwu – Ben-Farah, Mohamed A. – Hindy, Hanan – Bures, Miroslav – Atkinson, Robert – Tachtatzis, Christos – Andonovic, Ivan – Bellekens, Xavier (2022): Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information,* 13(3). Online: https://doi.org/10.3390/info13030146

Weston, David (2024): Helping our Customers through the CrowdStrike Outage. *Official Microsoft Blog,* 20 July 2024. Online: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

Zanni, John (2018): Ransomware Attack against Bristol Airport Shows Need for Smart, Secure Digital Infrastructure in Transportation. *Acronis,* 19 September 2018. Online: www.acronis.com/en/blog/posts/ransomware-attack-against-bristol-airport-shows-need-smart-secure-digital-infrastructure/

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 1. szám 57–75.
DOI: 10.32567/hm.2026.1.4

Pozderka Gábor[1]

A kibertér sajátosságából adódó civil–katonai kapcsolatok vizsgálata

Examination of Civil-Military Relations Arising from the Specificity of Cyberspace

Absztrakt

A civil–katonai kapcsolatok már a civilizációk kialakulásának kezdeti szakaszában is jelen voltak, irányaikat kijelölték az adott korszakra jellemző uralkodói és társadalmi elvárások. Jelen publikáció célja annak a folyamatnak a vizsgálata, hogy a 20. és 21. században kialakult civil–katonai kapcsolatok milyen módon alakultak át a kibertérben felerősödő folyamatok hatására, illetve a jövőben milyen speciális feladatokra kell felkészülnie a katonai szektornak a műveleti feladat-végrehajtás sikeressége érdekében. A civil szektor támogatása nélkül a jelen kor katonai műveletei már nem hajthatók végre, ennek érdekében a szükséges együttműködési platformokat ki kell alakítani, a közös feladat-végrehajtás kereteit ki kell dolgozni. Kiemelt figyelmet kell fordítani a folyamatok begyakoroltatására, ennek érdekében közös nemzeti és nemzetközi gyakorlatok tervezése és végrehajtása szükséges.

Kulcsszavak: civil–katonai kapcsolatok, kibertér, együttműködés, információmegosztás

Abstract

Civil-military relations were already present in the early stages of the formation of civilisations, and their directions were determined by the characteristics of the ruler and social expectations of the given era. The aim of this publication is to examine the process of how civil–military relations transformed in the 20th and 21st centuries as a result of the intensifying processes in cyberspace, and what special tasks the military sector should prepare for in the future

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

in order to be successful in the execution of operational tasks. Without the support of the civilian sector, the military operations of the present era can no longer be carried out, and in order to achieve this, the necessary cooperation platforms must be established and the framework for joint task execution must be developed. Special attention must be paid to the practice of the processes, for which joint national and international practices must be planned and implemented.

Keywords: civil–military relations, cyberspace, cooperation, information sharing

Bevezetés

Az információs és kommunikációs technológiák rohamos fejlődése az elmúlt évtizedekben alapjaiban formálta át a nemzetbiztonsági környezetet. A kibertér nem csupán új műveleti térként jelent meg, hanem olyan komplex térként, ahol a katonai és civil szereplők kapcsolatrendszere, döntéshozatali mechanizmusai és stratégiai tervei alapjaiban változtak meg.[2] Míg a hagyományos hadszíntéren a szereplők hierarchikus, jól meghatározott viszonyok alapján működtek, a kibertérben a határok elmosódnak, a szereplők változatosak és gyakran nehezen beazonosíthatók. Ez a környezet komoly kihívás elé állítja a civil–katonai kapcsolatok hagyományos modelljeit. Az évszázadok során kialakult CIMIC,[3] amely eddig főként békeműveletek és válságkezelés során bizonyított, a digitális térben újfajta adaptációt igényel az új típusú kihívások hatékony kezelése érdekében. Tradicionálisan a CIMIC szerepe abban áll, hogy a civil infrastruktúra, a humanitárius szervezetek, helyi hatóságok és más nem katonai szereplők működését összhangba hozza a katonai tevékenységekkel, különösen válságkezelési és konfliktusmegoldási környezetben.[4] A 21. század digitális kihívásai új dimenziókat adtak ehhez a hagyományosan fizikai térben működő szakterülethez. A tanulmány célja, hogy feltárja a kibertér sajátosságait, bemutassa a civil–katonai kapcsolatok átalakulását, és javaslatot adjon arra, hogy a CIMIC az információs műveletek részeként miként tud hatékonyan alkalmazkodni a kibertér követelményeihez, miközben biztosítja a katonai célok és a társadalmi érdekek egyensúlyát.

A kibertér, amely magában foglalja az információs és kommunikációs rendszereket, hálózatokat és adatfeldolgozó egységeket, egyre fontosabb operatív környezetté válik nemcsak a katonai, hanem a civil szereplők számára is – különösen mivel a kritikus infrastruktúra[5] és a közszolgáltatások nagymértékben függenek a digitális rendszerektől.[6] A kibertér működését a hagyományos hadszíntértől alapvetően három tényező különbözteti meg: a téridő nemlinearitása, a technológiák kettős felhasználhatósága és a szereplők sokszínűsége. Ezen tényezők hatékony kezelése és integrálása a korábban kialakított eljárásrendekbe nélkülözhetetlen érdek a siker érdekében, az erőforrás-menedzsment részeként szükséges megvizsgálni a meglévő erőforrások egy időben történő felhasználását, szükség szerint újrafelosztását.

[2] Clarke–Knake 2019.
[3] CIMIC, Civil–Military Cooperation.
[4] NATO Standardization Office 2025.
[5] Hunorfi–Farkas 2025.
[6] Haig 2023.

A kibertér sajátosságai

A téridő dimenzió elmosódása azt jelenti, hogy egy kibertámadás vagy információáramlás percek alatt globálisan hat, függetlenül a földrajzi elhelyezkedéstől, a rendszer viselkedése bonyolultabb, és kis változások is okozhatnak nagy vagy váratlan hatásokat. Ez a sajátosság alapvetően változtatja meg a stratégiai tervezést, hiszen a hagyományos logika, miszerint a fenyegetések fizikailag pontosan beazonosíthatók, a kibertérben már nem, vagy csak csekély mértékben érvényesek.

A technológiai eszközök kettős felhasználása szintén bonyolítja a helyzetet. Egyes platformok és szoftverek egyszerre szolgálhatnak katonai és civil célokat, legyen szó adatfeldolgozásról, kommunikációról vagy fenyegetésfelderítésről. Ez a kettős jelleg jogi, etikai és stratégiai kérdéseket vet fel, hiszen a civil felhasználásra szánt eszközök katonai alkalmazása felelősség- és hatáskörproblémákat generálhat. Ez a problémakör már a kezdeti lépéseknél megjelenik, hiszen a fejlesztések során felmerülhetnek olyan speciális katonai ágazati igények, amelyek a civil szektor részére nem jelentenek prioritást, így erőforrásokat szükséges átcsoportosítani, esetlegesen elvonni. A gyors technológiai fejlődés és a folyamatos innováció miatt a védekezési mechanizmusok is állandóan változnak. Amit ma hatékony védelemnek tekintünk, az rövid időn belül elavult lehet. Ez különösen a kritikus infrastruktúrák védelmében és a katonai információbiztonság terén jelent komoly kihívást. A civil és katonai szervezeteknek folyamatosan frissíteniük kell eljárásrendjeiket, és rendszeres képzéseket, gyakorlatokat kell biztosítaniuk a személyzet számára, természetesen ennek érdekében biztosítani kell a források rendelkezésre állását.

A szereplők sokszínűsége a kibertérben azt jelenti, hogy nemcsak állami szereplők, hanem magánvállalatok, civil kutatóintézetek, önkéntes csoportok és hacktivisták[7] is képesek befolyásolni a nemzetbiztonsági helyzetet. A civil szereplők között találjuk a kritikus infrastruktúrákat üzemeltető vállalatokat, informatikai cégeket, kutatóintézeteket, nonprofit szervezeteket és különböző szakmai közösségeket, míg a katonai oldalon a fegyveres erők és a nemzetbiztonsági szervezetek biztosítják a stratégiai felügyeletet és a reagálást. A képet tovább árnyalja, hogy egyes szeplők szerepkörei keveredhetnek egymással, a megszerzett tudás birtokában akár szerepkört is válthatnak, amivel alapjaiban változtathatják meg a korábban kialakult erőviszonyokat. Egy támadás forrása gyakran nehezen azonosítható, a motivációk és a hatások pedig összetettek.[8] A civil–katonai kapcsolatokban ezért olyan mechanizmusokat kell kialakítani, amelyek figyelembe veszik e sokszereplős környezetet, és lehetővé teszik a hatékony koordinációt, az információmegosztást és a gyors reagálást a fenyegetésekre.

Civil–katonai kapcsolatok a kibertérben

A civil–katonai kapcsolatok hagyományosan a békeműveletek, válságkezelés és humanitárius segítségnyújtás során a hatékony koordinációt, információmegosztást

[7] Krasznay 2024.
[8] Deibert 2003.

és erőforrás-optimalizálást szolgálják. A kibertérben azonban a kapcsolatok új jelentést kapnak, ez a folyamat a digitalizáció elterjedésével már korábban megkezdődött, a civil IT és logisztikai szolgáltatók már jelenleg is szoros kapcsolati hálót alakítottak ki a katonai ágazattal, nélkülük a kommunikáció és logisztikai ellátás már elképzelhetetlen. A katonai és civil szereplők közötti kommunikáció és együttműködés gyorsasága és pontossága élet-halál kérdése lehet, hiszen egy kibertámadás percek alatt jelentős károkat okozhat, legyen szó állami rendszerek, kritikus infrastruktúrák vagy magáncégek működésének megbénításáról.

A közös szabványok és protokollok kialakítása elengedhetetlen, mivel a civil és katonai szervezetek működési mechanizmusai eltérők, összehangolásuk nélkül a hatékony válaszadás nem biztosítható. Emellett a képzés és tudatosság növelése is nélkülözhetetlen. A kibertér folyamatosan változó fenyegetései miatt a szereplőknek rendszeresen kell gyakorolniuk a reagálást, szimulációkat végezniük, és közös munkacsoportok keretében fejleszteni a kommunikációs készségeket. A civil–katonai együttműködés tehát nem csupán technikai vagy stratégiai kérdés, hanem folyamatos emberi és szervezeti tanulási folyamat is.

A hagyományos CIMIC-hálózatok hierarchikus, lineáris kapcsolati struktúrákra épültek, ahol a feladatok és felelősségek jól meghatározottak voltak. A kibertér azonban ezzel szemben dinamikus, gyorsan változó és sokszereplős, így a CIMIC-nek alkalmazkodnia kell ehhez a környezethez. A megújulási folyamat részeként, nem csupán új eljárásrendekre van szükség, hanem egy olyan működési szemléletre, amely képes kezelni a valós idejű fenyegetéseket, integrálni a különböző szereplők tapasztalatait és biztosítani a gyors, koordinált válaszlépéseket.[9] A CIMIC jövőbeni szakértőinek így kettős kompetenciával kell rendelkezniük: egyszerre kell érteniük a hagyományos civil–katonai együttműködés működéséhez és a kiberműveletek sajátosságaihoz. Csak így képesek hidat képezni a katonai célok és a társadalmi érdekek között, miközben a civil lakosság és a kritikus infrastruktúrák védelme is biztosított marad.[10] A CIMIC szerepe a kibertérben tehát nem csupán koordinációs, hanem stratégiai is: az adaptív, hálózatszerű működés lehetővé teszi, hogy a civil és katonai szereplők integrált, rugalmas kiberhálóban működjenek együtt, amely gyorsan alkalmazkodik a folyamatosan változó fenyegetésekhez. A cél ezzel egyértelmű: olyan civil–katonai kiberháló kialakítása, amely elősegíti a közös kiberbiztonsági tudatosságot, növeli a rezilienciát, és hosszú távon fenntartható módon biztosítja a katonai célok és a társadalmi igények egyensúlyát.[11]

Civil és katonai szereplők a kibertérben

A kibertér civil szereplői rendkívül sokszínűek, és tevékenységük közvetlenül vagy közvetve befolyásolja a nemzetbiztonságot. A kritikus infrastruktúrákat üzemeltető vállalatok elsőként érzékelhetik a kibertámadásokat, legyen szó energiaellátásról,

[9] NATO Standardization Office 2025.
[10] NATO CIMIC Centre of Excellence 2025b.
[11] Kott et al. 2018.

közlekedési rendszerekről vagy kommunikációs hálózatokról. Ők rendelkeznek azzal a technikai szakértelemmel és adatokkal, amelyek lehetővé teszik a támadások gyors azonosítását és a hatékony reagálást. Ugyanakkor nem csak a nagyvállalatok számítanak aktív szereplőnek; a kutatóintézetek és egyetemek például folyamatosan fejlesztik a fenyegetés felderítéséhez szükséges módszereket, modellezik a kibertámadások hatásait, és így közvetlenül járulnak hozzá a kiberbiztonsági innovációhoz. Nonprofit szervezetek, szakmai közösségek és hacktivista csoportok pedig gyakran reagálnak gyorsabban, mint a formális állami struktúrák, különösen az incidensek korai szakaszában. Ez a sokszínűség előnyökkel és kihívásokkal is jár. A civil szereplők gyakran nem kötődnek központi parancsstruktúrához, és működésük eltérő szabályok, jogi és etikai keretek szerint zajlik. A katonai és állami szervezeteknek ezért rugalmasan kell kezelniük ezeket az interakciókat, miközben biztosítaniuk kell a gyors információáramlást és a koordinált reagálást.

A katonai és nemzetbiztonsági szervezetek feladata a kibervédelemben elsősorban a stratégiai tervezés, a fenyegetések azonosítása és a gyors reagálás biztosítása. Ők képezik a struktúrát, amely a különböző civil információforrásokat rendszerezi és integrálja a védelmi mechanizmusokba. A katonai szereplőknek a kibertérben nem elég a hagyományos parancs-irányítási logikát követniük, mert a fenyegetések gyorsan változnak, és sok esetben decentralizált vagy nem állami szereplőktől erednek. Ebben a környezetben a koordinációs mechanizmusok rendkívül fontosak. Például egy kritikus infrastruktúrát ért támadás esetén a civil üzemeltetők adatait össze kell hangolni a katonai fenyegetésfelderítéssel és az állami reagálási protokollokkal. A koordináció célja, hogy minden résztvevő számára világos legyen a szerepe, ugyanakkor a döntéshozatal gyors és adaptív maradjon. E mechanizmusok közé tartozik a közös incidenskezelési protokollok kidolgozása, valós idejű információcsere, valamint a rendszeres közös gyakorlatok és szimulációk szervezése. Fontos kialakítani a bizalmi hálót és biztonságos technikai platformokat, ellenkező esetben a hatékony reagálás nem lesz lehetséges.

A civil és katonai szereplők együttműködésének gyakorlati modelljei különbözők lehetnek. Egyes esetekben központi koordináció érvényesül, ahol állami vagy katonai egység gyűjti össze a civil és katonai információkat, elemzi azokat, és koordinált válaszlépéseket kezdeményez együttműködésben a civil szereplőkkel. Ez a modell előnyös a stratégiai irányítás és a konszolidált döntéshozatal szempontjából, ugyanakkor korlátozott rugalmassággal rendelkezik, különösen a helyi incidensek gyors kezelésében. Más esetekben decentralizált, hálózatszerű működés alakul ki, ahol a civil és katonai szereplők közvetlenül kommunikálnak egymással. Itt a koordinációs mechanizmusok segítő jellegűek, a hangsúly a gyors reagáláson, a helyi adaptáción és a folyamatos információmegosztáson van. Ez a modell előnyös a gyors fenyegetésfelderítésnél és az innovatív megoldások alkalmazásánál, ugyanakkor nagyobb felelősséget követel a résztvevőktől, mivel a döntések decentralizáltak. A gyakorlatban gyakran hibrid megoldások alkalmazhatók,[12] amelyek kombinálják a központi koordináció előnyeit a hálózatszerű rugalmassággal. Ebben a struktúrában a CIMIC például szerepelhet a civil–katonai koordináció egyik elemeként, de nem kizárólagos mechanizmusként,

[12] Resperger–Kiss–Somkuti 2014.

hanem a partnerségi kapcsolatok és információmegosztás biztosítására. A hangsúly azonban a rendszer sokszereplős, adaptív jellegén van, ahol a katonai és civil szereplők egyenrangú, de különböző funkciókkal rendelkező partnerek. Az azonban minden esetben kijelenthető, hogy a kapcsolati háló kialakítása és naprakészen tartása, valamint a folyamatok készségszintű begyakorlása kulcsfontosságú lesz a feladat-végrehajtás során; ha ez nem történik meg egy esemény bekövetkezése előtt, akkor arra az esemény kezelése közben már nem lesz lehetőség.[13]

Az országok katonai kiberparancsnokai kulcsszereplők a modern hadsereg és a kormányzat digitális biztonságának fenntartásában. Ez a funkció mind a NATO, mind az EU[14] esetében a nemzetek által dedikált funkcióként jelenik meg. Elsődleges feladatuk a katonai kibertér műveleti erők irányítása és koordinálása.[15] Ugyanakkor szerepük messze túlmutat a katonai műveleteken, és szoros kapcsolatot igényel a civil szektorral. A kiberparancsnokok gyakran kapcsolatot tartanak a polgári kormányzati szervekkel, például a belügyi tárcákkal, hírszerző ügynökségekkel vagy a kritikus infrastruktúrák üzemeltetőivel. Ez a kapcsolat biztosítja, hogy a civil döntéshozók időben értesüljenek a kiberfenyegetésekről, az információáramlás és a figyelmeztetések kulcsfontosságúak a hatékony védelemhez. Válsághelyzetekben, például kibertámadások során, a kiberparancsnok feladata a katonai és civil reagálás összehangolása. A civil szervek gyakran nem rendelkeznek a támadások elleni speciális tapasztalattal vagy erőforrásokkal, így a katonai kibererők támogatása elengedhetetlen. A parancsnok biztosítja, hogy a válsághelyzetben minden érintett fél egy koordinált stratégiát kövessen. Ezzel csökkenthető a károk mértéke és gyorsítható a helyreállítás, emellett stratégiai tanácsadóként is működik a kormányzat számára. Elemzi a fenyegetéseket, és javaslatokat ad a szükséges védelmi intézkedésekre, így a civil döntéshozók tudatosan és reálisan mérhetik fel a kiberkockázatokat. A katonai kiberparancsnokok szerepe azonban nem csupán reagáló, hanem megelőző jellegű is. Részt vállalnak a civil szakemberek képzésében és tudatosságuk növelésében, ezzel elősegítve, hogy a polgári szervezetek jobban felkészüljenek a potenciális támadásokra. A parancsnokok segítik a kommunikációs csatornák kialakítását a civil és katonai szervezetek között, ez a kapcsolat lehetővé teszi az információ gyors és pontos cseréjét. A kiberparancsnok szerepe ezért alapvető a bizalom és az együttműködés erősítésében is, részt vesz a kiberbiztonsági stratégia kidolgozásában és frissítésében. A katonai és civil szféra közötti koordináció különösen fontos a kritikus infrastruktúrák védelmében. Az áram-, víz- vagy pénzügyi rendszerek elleni kibertámadások gyors és hatékony reagálást igényelnek, ezen infrastruktúrák rendelkezésre állása számos esetben szintén elengedhetetlen a katonai műveletek sikeres végrehajtásához, ennek érdekében a parancsnok biztosítja, hogy a katonai erők támogassák a civil védelmet. A kibertér műveleti erők feladata, hogy a katonai és civil műveletek összhangban legyenek, és az erőforrások hatékonyan legyenek felhasználva. A fenti szempontokat figyelembe véve a katonai kiberparancsnokok tevékenysége így egyszerre stratégiai, taktikai és koordinációs jellegű feladat.

[13] Balogh 2025.
[14] The Joint Cyberspace Command Participates In The Cyberco 2024.
[15] 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről.

A fenti elemzésből láthatjuk, hogy a kibertér civil–katonai kapcsolatai komplexek, dinamikusak és folyamatosan változnak. A civil szereplők technológiai tudása és gyors reagálása, valamint a katonai szervezetek stratégiai irányítása és koordinációs képessége együtt teremthet hatékony védelmet és gyors reagálást a kibertámadásokkal szemben. A CIMIC ebben a kontextusban egy példa a koordinációra mint meglévő képesség, de nem az egyetlen lehetséges forma, azonban érdemes megvizsgálni az abban rejlő lehetőségeket. A sikeres együttműködés kulcsa az interoperabilitás, a bizalom, az információáramlás gyorsasága és a szereplők folyamatos adaptációs képessége.

Nemzetközi keretek és gyakorlatok

A kibertér globális jellege miatt a civil–katonai kapcsolatok nem csupán nemzeti szinten értelmezhetők. A kibertámadások hatásai gyorsan átléphetik az államhatárokat, és a felelősség, a reagálás és a védelem gyakran nemzetközi együttműködést igényel.[16] Ebből következően a civil és katonai szereplők közötti koordináció nemcsak belső struktúrákon alapul, hanem a nemzetközi jogi, szabályozási és stratégiai keretek figyelembevételével is. A kibertérben történő műveletek jogi szabályozása komplex feladat, mert egyszerre kell figyelembe venni a nemzetközi humanitárius jogot, az államok szuverenitását, valamint a polgári és katonai szereplők tevékenységét. A nemzetközi egyezmények, például az ENSZ Alapokmányának[17] vonatkozó rendelkezései, az EU kibervédelmi irányelvei (NIS/NIS2,[18] Cybersecurity Act, GDPR[19]) vagy a NATO kiberbiztonsági protokolljai[20] meghatározzák a katonai műveletek kereteit, és alapot biztosítanak a civil–katonai együttműködéshez. A jogi keretek szerepe kettős, egyrészt biztosítják a tevékenységek törvényességét, másrészt elősegítik a felelősség és hatáskör egyértelmű meghatározását. Például egy kritikus infrastruktúrát ért kibertámadás során világosan definiálni kell, hogy mely állami szervek, katonai egységek vagy civil cégek jogosultak beavatkozni, és milyen eljárásrend szerint történik az incidens kezelése.

Számos nemzetközi példa mutatja, hogy a civil és katonai szereplők hatékony együttműködése a kibertérben lehetséges, ha jól definiált koordinációs mechanizmusok léteznek. A NATO kiberbiztonsági kezdeményezései, például a Cooperative Cyber Defence Centre of Excellence (CCDCOE), lehetővé teszik, hogy a tagállamok katonai és civil szervei közös szimulációkban és gyakorlatokban vegyenek részt, így javítva a koordinációt és a gyors reagálást. Az EU szintén folyamatosan fejleszti a civil–katonai koordinációt, különösen a kritikus infrastruktúrák és kiberincidensek kezelésében. A közös adatbázisok, fenyegetésfigyelő rendszerek és valós idejű információmegosztási platformok lehetővé teszik, hogy a civil és katonai szereplők gyorsan reagáljanak a fenyegetésekre, és minimalizálják a károkat. Nem minden együttműködési modell centralizált, sok esetben hálózatszerű, decentralizált megoldások bizonyultak hatékonynak.

[16] Bencsik–Karpiuk 2021.
[17] United Nations [é. n.].
[18] Network and Information Security Directive, NIS.
[19] General Data Protection Regulation, GDPR.
[20] NATO Standardization Office 2020.

A nemzetközi gyakorlatban több eset bizonyítja, hogy a civil–katonai koordináció elengedhetetlen a kibervédelemben. Az EU-ban történt kiberincidensek kezelésében a civil szolgáltatók és katonai elemzők közös munkacsoportokat hoztak létre, amelyek koordináltan azonosították a fenyegetést, és előkészítették a válaszlépéseket. Hasonló mechanizmusokat alkalmaz a NATO a baltikumi országokban a kritikus infrastruktúra védelmére irányuló gyakorlatok során. Ezek a példák rámutatnak arra, hogy a sikeres koordináció nem csupán a technológiai eszközökön múlik, hanem a szervezeti kultúrán, a kommunikációs csatornákon és a jogi kereteken is. A civil és katonai szereplők közötti bizalom, az információmegosztás gyorsasága és a közös szimulációkban szerzett tapasztalatok kritikus tényezők a hatékony reagálás szempontjából.

Ebben a kontextusban a CIMIC-szakterület esetében figyelembe kell venni, hogy a kiberbiztonság nem csupán technikai kérdés, hanem a civil társadalom és a katonai erők együttműködésének új terepe.[21] A NATO CIMIC Centre of Excellence (CCOE) hangsúlyozza, hogy a hibrid fenyegetések kezelése – beleértve a kiberincidenseket – csak úgy lehetséges, ha a civil és katonai elemzők, döntéshozók és végrehajtók közösen dolgoznak a reziliencia növelésén és a fenyegetések csökkentésén. A CCOE szakmai műhelyei, tanulmányai és esettanulmányai rámutatnak arra, hogy a kiber- és információs műveletek hatással vannak a CIMIC operatív célokra, és ezeket a hatásokat a CIMIC elemzési kereteibe és gyakorlatába integrálni szükséges. Nemzetközi gyakorlatban ez a felismerés különböző szinteken valósul meg. A NATO-tagállamok és -partnerszervezetek együttműködnek a kiberbiztonsági képzésben, közös gyakorlatokban és információmegosztási mechanizmusokban, amelyek célja a civil és katonai szereplők közötti interoperabilitás erősítése a kiberdimenzióban is. Az Európai Unió és a NATO közötti kibervédelmi konzultációk, amelyek a diplomáciai és katonai kiberparancsnokok között jöttek létre, szintén a civil–katonai koordináció gyorsabb és hatékonyabb működésére irányulnak a kiberfenyegetésekkel szemben. A CIMIC klasszikus feladatai – mint a humanitárius segítség koordinálása vagy a civil kritikus infrastruktúra védelmének támogatása – ma már egyre inkább kiegészülnek olyan elemekkel, amelyek a digitális infrastruktúra biztonságát, az információbiztonságot és a kiberrezilienciát is magukba foglalják. Ez a bővülő szerep azonban nem jelenti a CIMIC katonai kiberműveleti tevékenységgé válását, hanem azt a felismerést tükrözi, hogy a modern válságok és konfliktusok nem választják szét a fizikai és digitális dimenziókat, a civil lakosságot, infrastruktúrát és intézményeket érintő kiberfenyegetések kezelése alapvető része a hatékony civil–katonai együttműködésnek is.[22] A NATO megfogalmazása szerint: a CIMIC „must be recognized in every domain of operations and in all effects dimensions — physical, virtual, and cognitive", ami alátámasztja, hogy nem a katonai kiberhadviselés kiszélesítéséről van szó, hanem a civil tényezők beemeléséről a kiberbiztonsági szemléletbe. Más szóval, a NATO a gyakorlatban is érvényesíti azt az elvet, hogy a modern válságkörnyezetben a fizikai és digitális tér egymásra hatása miatt a CIMIC feladata a civil társadalom kibertérben való védelmének támogatása. A NATO Allied Command Transformation (ACT) 2025-ös elemzése szerint[23] a CIMIC

[21] Varga 2022.
[22] NATO CIMIC Centre of Excellence 2025c.
[23] NATO's Strategic Warfare Development Command 2025.

COE kulcsszerepet játszik abban, hogy a NATO erői képesek legyenek a civil tényezők integrálására a műveleti tervezésbe, különösen a komplex, hibrid fenyegetésekkel terhelt környezetben. A dokumentum rámutat, hogy a modern műveletekben a civil infrastruktúra elleni kibertámadások gyakran nagyobb hatással vannak a műveletek sikerére, mint a hagyományos katonai fenyegetések. A CIMIC feladata, hogy a civil szereplőkkel együttműködve feltárja a kritikus infrastruktúrák sérülékenységeit, és biztosítsa a katonai műveletekhez szükséges feltételeket. A NATO ACT szerint a CIMIC nem válik kiberműveleti szerepkörré, de a civil környezet digitális sérülékenységeinek kezelése nélkülözhetetlen a műveleti sikerhez. Az elemzés hangsúlyozza, hogy a civil és katonai szereplők közötti együttműködés ma már a kibertérben is elengedhetetlen, mivel a civil rendszerek elleni támadások közvetlenül befolyásolják a katonai műveletek végrehajtását. Ez a megközelítés jól illeszkedik ahhoz a felismeréshez, hogy a modern válságok nem választják szét a fizikai és digitális dimenziókat.

A nemzetközi példák közül kiemelhető a CIOR CIMEX (Civil–Military Exercise)[24] a NATO tartalékos tisztjeit tömörítő CIOR éves, többnapos civil–katonai együttműködési gyakorlata, amely 2012 óta készíti fel a résztvevőket összetett válsághelyzetek kezelésére. A gyakorlat *table top* formában zajlik, és olyan többdimenziós NATO-műveleti környezetet modellez, ahol a civil hatóságokkal, intézményekkel és infrastruktúrákkal való koordináció kulcsfontosságú. A szcenáriók között rendszeresen megjelennek kibertámadásokkal kombinált krízisek, például árvíz vagy tömeges migráció esetén fellépő digitálisinfrastruktúra-zavarok. Ezekben a helyzetekben a CIMIC feladata nem a kiberműveletek végrehajtása, hanem a civil lakosságot és szolgáltatásokat érintő hatások elemzése és a helyreállítás támogatása. A CIMEX gyakorlatai szintén alátámasztják, hogy a modern válságokban a fizikai és digitális dimenziók elválaszthatatlanok. A civil infrastruktúrát érő kiberfenyegetések kezelése ezért ma már a hatékony CIMIC-tevékenység alapvető részét kell hogy képezzék, anélkül, hogy a CIMIC kiberműveleti szerepkörré válna. Ez a nemzetközi példa pontosan alátámasztja azt a felismerést, hogy a civil–katonai együttműködésnek ma már a digitális térben jelentkező fenyegetésekre is reagálnia kell.

Magyarországhoz hasonlóan Németországban is megkezdődött a kiber- és információs műveleti képességek átstruktúrálása egy szervezetbe. Ennek részeként a Bundeswehren belül a Cyber- und Informationsraum (CIR) nevű önálló szervezetben összpontosulnak ezen képességek, amely szervezet felel a kiber- és információs műveletekért, továbbá a kapcsolódó felderítési feladatokért is. Bár jelenleg a CIMIC képesség a Joint Support Command alárendeltségében működik, a Bundeswehr műveleti tervezési és végrehajtási rendszerében a két terület szoros együttműködésben dolgozik, különösen többdimenziós *(multidomain)* műveletek esetén. A CIR biztosítja a digitális és információs környezet feletti műveleti képességeket, míg a CIMIC a civil szereplőkkel, hatóságokkal és szervezetekkel való koordinációt végzi. A német modell eljárási és műveleti szinten valósítja meg az integrációt, az elkövetkező időszakban elemzik annak hatékonyságát, és a tapasztalatok figyelembevételével tesznek további javaslatokat az esetleges további integrációra.

[24] Lásd: https://cior.net/activities/civil-military-exercise/

Az USA-ban használt gyakorlat lényege, hogy a Civil Affairs (CA) – amely a CIMIC amerikai megfelelője – és a kiberműveleti szervek együttműködése nem különálló feladat, hanem a teljes műveleti ciklusba beépített eljárásrend. Az USA kiberstratégiája[25] a civil és katonai szereplők összehangolt működését alapkövetelményként határozza meg, mivel a kibertámadások elsődleges célpontjai jellemzően civil infrastruktúrák, amelyeket a hadsereg önmagában nem tud megvédeni. A CA feladata ezért az, hogy kapcsolatot tartson a kritikus infrastruktúrák üzemeltetőivel, felmérje a kibertámadások civil hatásait, és közvetítse ezeket a katonai kiberparancsnokság felé. A NATO Cyber Coalition gyakorlatok amerikai részvétele is azt mutatja, hogy a CA és a kibererők közösen dolgoznak a helyzetértékelésen, a civil szolgáltatások helyreállításán és a lakosság tájékoztatásán. A CCDCOE kutatásai alapján az amerikai modell egyik sajátossága, hogy a kiberfenyegetések kezelésébe rendszeresen bevonja a magánszektort is, különösen a technológiai vállalatokat és az infrastruktúra-üzemeltetőket, ami a CIMIC-szemlélet digitális kiterjesztésének tekinthető. A CA és a Cyber Command közötti együttműködés így nem *ad hoc,* hanem intézményesített: közös helyzetértékelés, információmegosztás, civil hatásvizsgálat és válságkezelési koordináció formájában jelenik meg. A NATO-val közös amerikai gyakorlatok azt is megerősítik, hogy a CA-egységek kulcsszerepet játszanak a civil lakosság rezilienciájának fenntartásában kibertámadások idején, például az energia- vagy egészségügyi rendszerek sérülésekor. Összességében megállapítható, hogy az amerikai eljárásrend lényege, hogy a CA a kiberhadviselésben kapcsolati és koordinációs csomópontként működik, amely összeköti a katonai kiberképességeket a civil infrastruktúrákkal, a helyi hatóságokkal és a lakossággal. Ez a modell a NATO-ban is iránymutatónak számít, és a kiberfenyegetések növekedésével várhatóan tovább erősödik majd, a Magyar Honvédség a gyakorlatok során megkezdte ennek a modellnek a tesztelését és rendszerbe történő integrálását.

A nemzetközi példák és jogi keretek azt mutatják, hogy a civil–katonai kiberkoordináció lehetséges, de csak akkor, ha a szereplők képesek adaptálódni a gyorsan változó fenyegetésekhez, és rugalmasan kezelik az együttműködést; a hangsúly a szereplők közötti partnerségen, a gyors információáramláson, a jogi és etikai kereteken, valamint a folyamatos tanuláson van. A globális kiberfenyegetések egyre összetettebbé válnak, ezért a civil–katonai kapcsolatok nem csupán operatív, hanem stratégiai szinten is kulcsfontosságúak. A tapasztalatok azt mutatják, hogy a hatékony együttműködés alapja a világos szerepkörök, a közös gyakorlatok, a bizalom és az interoperabilitás, amelyek lehetővé teszik, hogy a civil és katonai szereplők egységes, adaptív hálózatként reagáljanak a kibertámadásokra.

Magyarországi civil–katonai kiberkoordináció

Magyarországon, mint a legtöbb NATO- és EU-nemzet esetében, a kibertér védelme és a civil–katonai együttműködés egyre nagyobb hangsúlyt kap, különösen az állami,

[25] White House 2026.

katonai és kritikusinfrastruktúra-szereplők között. A hazai Nemzeti Biztonsági Stratégia[26] és más ágazati stratégiai szintű dokumentumok kiemelten foglalkoznak a kiberbiztonsággal. A polgári és katonai szervezetek közötti kiberkoordinációs együttműködés a kiberbiztonság és kibervédelem területén több szinten és intézményrendszerben valósul meg. Magyarország jogi szabályozással támogatja a kiberbiztonsági tevékenységek koordinációját, 2024-ben hatályba lépett a magyar kiberbiztonságról szóló törvény[27] és annak végrehajtási rendelete, amely előírja a nemzeti kiberbiztonsági munkacsoport létrehozását. Ennek a testületnek feladata a kiberbiztonsági politika koordinálása, amelyben mind az állami, mind a magánszektor, továbbá a polgári és katonai szervezetek képviselői részt vesznek. A szabályozás nemzeti kapcsolattartó pontot is kijelöl, amely a határon átnyúló kibervédelem és incidenskezelés során az információcserét koordinálja. Ezek a dokumentumok jogi alapot és stratégiai irányt adnak arra, hogyan kell integrálni a polgári és katonai kapacitásokat a kibervédelemben.

Magyarországon a polgári kiberbiztonsági koordináció központi szereplője a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NKI vagy National Cyber Security Center Hungary) mint kormányzati szervezet kiberbiztonsági támogatást nyújt a hazai közigazgatás és önkormányzati informatikai rendszerek védelméhez, illetve a civil szereplők biztonsági tudatosságának növeléséhez. Fontos elemként jelenik meg a Nemzeti Koordinációs Központ (NCC-HU), amely az EU kiberbiztonsági kompetenciahálózatának hazai csomópontja, feladatai közé tartozik a hazai civil szereplők – ipar, kutatás, oktatás, közszféra – tevékenységének összehangolása, projektfinanszírozás támogatása, tudásépítés és nemzetközi együttműködés elősegítése.

Honvédelmi ágazati szinten a Honvédelmi Minisztérium, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség különböző szervezeti egységei hajtanak végre szakterületük vonatkozásában kiberterületi koordinációt, amely a honvédelmi és nemzetközi kötelezettségeket szolgálja, valamint az igazságügyi, rendészeti és terrorelhárítási szervek, amelyek polgári és katonai információcserét is végeznek.

A civil szektor részéről a kritikus infrastruktúrák üzemeltetői, informatikai cégek és kutatóintézetek nyújtanak technikai szakértelmet és valós idejű információkat. A civil és katonai szereplők közötti együttműködés folyamatosan fejlődik, különösen a közös képzések, szimulációk és gyakorlatok révén. Magyarországon az oktatási intézmények fontos szerepet játszanak abban, hogy a civil és katonai szereplők a kiberbiztonság területén hatékonyan tudjanak együttműködni. A Nemzeti Közszolgálati Egyetem különleges helyzetben van, mivel egy intézményen belül készíti fel a honvédelmi, rendészeti, közigazgatási és nemzetbiztonsági területen dolgozó szakembereket, így a hallgatók már a képzés során megismerik egymás gondolkodásmódját, feladatait és működési kereteit. Ezt a megközelítést egészítik ki a műszaki és informatikai profilú egyetemek, például a Budapesti Műszaki és Gazdaságtudományi Egyetem és az Óbudai Egyetem, amelyek a kiberbiztonság technikai hátterét adják, valamint kutatási és fejlesztési munkájukkal közvetlenül is támogatják az állami és honvédelmi szervezeteket. A jogi és társadalomtudományi képzések szintén hozzájárulnak ahhoz, hogy a kibertérben zajló együttműködés jogszerű és felelős módon valósuljon meg.

[26] Kovács 2020.
[27] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

Az egyetemek emellett olyan szakmai találkozási pontokat is biztosítanak – konferenciák, képzések és közös gyakorlatok formájában –, ahol a civil és katonai szakemberek személyes kapcsolatokat építhetnek ki. Ezek a kapcsolatok a gyakorlatban megkönnyítik az információcserét és a közös fellépést, ami válsághelyzetben gyorsabb reagálást és kiszámíthatóbb együttműködést tesz lehetővé, ezáltal erősítve az ország ellenálló képességét a kibertérben. Tendenciaként megfigyelhető, hogy a honvédelmi ágazat gyakorlataiba, egyre inkább már a tervezés fázisában, is bevonják az egyetemi hallgatókat.

Magyarországon a civil–katonai szerepek adaptációja szoros összefüggésben áll a kibertér gyors változásaival. A katonai szervezeteknek rugalmasabbá kell válniuk, és alkalmazkodniuk kell a civil szektor gyors reagálásához és technológiai innovációihoz. Ugyanakkor a civil szereplők számára is létfontosságú, hogy megértsék a katonai és állami struktúrák működését, hogy a közös munkában ne alakuljon ki félreértés vagy késlekedés. A hazai civil–katonai kiberkoordináció és az összkormányzati gyakorlatok azt mutatják, hogy a kibertérben az együttműködés lehetőségei széles spektrumon mozognak. A siker kulcsa a gyakorlatias képzés, az interoperabilitás, az adaptáció és a bizalom, a valódi érték a szereplők közötti partnerségből és a folyamatos tanulásból származik, a feladatrendszer folyamatosan fejleszthető és kiegészíthető.

A tartalékos rendszer a kiber szakterület számára kifejezetten sok lehetőséget kínál a jövőben, mivel a kibervédelemben szükséges tudás és tapasztalat jelentős része a civil szférában halmozódik fel, különösen az informatikai és távközlési területeken. A rendszer egyik legnagyobb előnye, hogy lehetővé teszi magasan képzett szakemberek bevonását anélkül, hogy hosszú távon el kellene őket vonni a civil munkahelyüktől, így az állam és a honvédség hozzáférhet a legfrissebb technológiai ismeretekhez és piaci tapasztalatokhoz. A kibetartalékosok révén gyorsan bővíthetők az erőforrások válsághelyzetben vagy megnövekedett fenyegetettség idején, miközben békeidőben a rendszer fenntartása kisebb költséggel jár, mint egy teljesen hivatásos állományé. Emellett a tartalékos szolgálat hidat képez a civil és katonai szféra között, mivel az érintett szakemberek mindkét környezet működését ismerik, és képesek közvetíteni az eltérő szervezeti kultúrák és eljárások között. A célzott kiképzések és gyakorlatok révén a tartalékos állomány bekapcsolható incidenskezelési, elemzési vagy tanácsadói feladatokba, ami növeli a rendszer rugalmasságát és alkalmazkodóképességét. Összességében kijelenthető, hogy a kiberszakterülethez illesztett tartalékos rendszer hozzájárulhat a nemzeti kiberreziliencia erősítéséhez, mivel egyszerre növeli a szakmai kapacitást, csökkenti a kiszolgáltatottságot, és javítja a civil–katonai együttműködés gyakorlati működését.

Jogi kérdések és javaslatok a civil–katonai kiberkoordináció feladataira

A kibertér sajátosságai és a civil–katonai kapcsolatok vizsgálata rávilágítanak arra, hogy a hagyományos állami és katonai struktúrák önmagukban nem képesek teljes mértékben kezelni a kibervédelmi fenyegetéseket.[28] A civil szereplők – a kritikus

[28] Ertan et al. 2020.

infrastruktúrát üzemeltető vállalatok, technológiai cégek[29] vagy kutatóintézetek – gyors reagálásukkal és szakértelmükkel jelentősen hozzájárulnak a kibervédelmi képességekhez. A korábbi pontokban bemutatott nemzetközi és hazai példák alapján világossá vált, hogy a civil–katonai koordináció nem pusztán technikai feladat, hanem szervezeti, stratégiai és jogi dimenziókat is magában foglal, amelyek összehangolt működés nélkül nem biztosítják a hatékony reagálást.

A vizsgálat során két fő jellegzetesség rajzolódott ki. Egyrészt a civil és katonai szereplők közötti interakció egyre inkább többszereplős, hálózatszerű rendszerré alakult, amely lehetővé teszi a gyors reagálást, ugyanakkor folyamatos koordinációt és tapasztalatcserét igényel. Az ilyen hálózatok előnye, hogy minden résztvevő azonnal hozzá tud járulni a fenyegetésfelderítéshez, és gyorsan be tudja vinni a saját szakterületi ismereteit a döntéshozatali folyamatokba. Másrészt a civil–katonai koordinációban a formalizált mechanizmusok, például az incidenskezelési protokollok és a jogi keretek biztosítják, hogy a felelősségi viszonyok világosak maradjanak, és a döntések jogszerűen történjenek.[30] A legjobb eredmény akkor születik, ha a decentralizált hálózatok rugalmassága és a formalizált koordinációs mechanizmusok egyaránt érvényesülnek.

Ugyanakkor a koordináció során több kihívással is szembesülünk. A bizalom és az adatmegosztás kérdése gyakran kritikus tényező, hiszen a civil szereplők érzékeny adatokat kezelnek, és nem minden esetben hajlandók azokat azonnal megosztani katonai vagy állami szereplőkkel. További nehézséget jelent a technológiai és képességbeli eltérés, ami miatt a civil és katonai szereplők nem mindig azonos szinten reagálnak az incidensekre, és a koordináció során késlekedések vagy félreértések léphetnek fel. A jogi keretek kulcsfontosságúak a civil–katonai együttműködésben, mivel meghatározzák, hogy milyen tevékenységek jogszerűek, milyen szereplők milyen mértékben avatkozhatnak be, és hogyan kezelhetők a polgári jogi szempontok. Ahogyan a korábbi fejezetekben már vizsgáltuk, nemzetközi jogi keretek között az ENSZ Alapokmánya és az államok közötti kiberműveletekre vonatkozó normák biztosítják az általános kereteket, míg a NATO és az EU kiberbiztonsági protokolljai és irányelvei konkrét útmutatást adnak a civil és katonai szereplők közötti információmegosztásra és incidenskezelésre. Magyarországon a hazai jogszabályok és az adatvédelmi szabályok biztosítják, hogy a civil–katonai koordináció jogszerű keretek között működjön, és a polgári érdekek ne sérüljenek. A jogi keretek nem csupán formális követelmények, hanem a civil–katonai együttműködés alapját is adják. Világossá teszik, hogy ki, mikor és milyen feltételekkel avatkozhat be egy incidens során, és biztosítják a felelősségi körök tisztaságát. A jogi megfelelés hozzájárul a bizalom kialakulásához, elősegíti az információmegosztást, és csökkenti az esetleges félreértésekből vagy visszaélésekből eredő kockázatokat.

[29] Bonnyai–Kiss–Tóth 2023.
[30] Szádeczky 2018.

Javaslatok és ajánlások a hatékonyabb civil–katonai kibertéri koordinációhoz

A vizsgálat és a gyakorlati tapasztalatok egyértelműen rámutatnak arra, hogy a civil–katonai kiberkoordináció fejlesztése nem egyetlen intézkedéssel, hanem egymásra épülő szervezeti, technológiai és humán lépések sorozatával érhető el.[31] Alább olyan javaslatok olvashatók, amelyek nemcsak elvi következtetéseket vonnak le, hanem konkrét, rövid távon is megvalósítható ajánlásokat fogalmaznak meg a hatékony rendszer kialakítása érdekében.

Interoperabilitás és technológiai kompatibilitás

A vizsgálat alapján megállapítható, hogy az eltérő technikai megoldások és információkezelési eljárások akadályozzák a gyors és pontos helyzetértékelést, ami válsághelyzetben közvetlenül rontja a reagálás hatékonyságát. Amennyiben a civil és katonai szereplők nem azonos vagy kompatibilis rendszereket használnak, az információáramlás megszakadhat vagy torzulhat.

Javaslat: indokolt egy közös technikai minimumkövetelmény-rendszer kialakítása, valamint olyan szabványosított adatmegosztási és kommunikációs felületek bevezetése, amelyek biztosítják a rendszerek közötti folyamatos interoperabilitást, ezeket nem elég kiépíteni, folyamatos karbantartást igényelnek.

Közös képzések és szimulációk

A tapasztalatok azt mutatják, hogy a koordináció hiányosságai leginkább éles helyzetben válnak láthatóvá, amikor már nincs lehetőség a szerepek és eljárások tisztázására. A rendszeres közös gyakorlatok hiánya növeli a bizonytalanságot és a döntési késedelmet.[32]

Javaslat: szükséges intézményesíteni az évente ismétlődő, civil–katonai részvétellel zajló kiberbiztonsági szimulációkat, amelyek során a résztvevők gyakorolhatják a közös döntéshozatalt, az információmegosztást és a jogi keretek gyakorlati alkalmazását. A katonai ágazat gyakorlataiba minél szélesebb körben kell bevonni a civil szereplőket.

Rugalmasság és adaptáció

A központosított irányítás önmagában nem képes kezelni a kibertér gyorsan változó és gyakran lokális jellegű fenyegetéseit. A túlzott centralizáció lassíthatja a reagálást, míg a teljes decentralizáció stratégiai széttagoltsághoz vezethet.

[31] Boeke–Heinl–Veendaal 2018.
[32] Krasznay–Hámornik 2019.

Javaslat: olyan hibrid koordinációs modellt szükséges kialakítani, amely stratégiai szinten központi irányítást biztosít, ugyanakkor operatív szinten felhatalmazza a helyi szereplőket az önálló, gyors döntéshozatalra, meghatározott keretek között. A kiberparancsnok és az MH kibertér műveleti erőinek feladat-végrehajtását integrálni kell ebbe a feladatrendszerbe, a civil szereplőknek ismerniük kell lehetőségeiket és feladatukat.

Bizalom és kommunikáció erősítése

Az elemzés rámutat arra, hogy a bizalom hiánya információ-visszatartáshoz és párhuzamos intézkedésekhez vezethet, ami jelentősen csökkenti az együttműködés hatékonyságát. A bizalom kialakulása azonban nem spontán folyamat, hanem tudatos szervezeti erőfeszítést igényel.

Javaslat: célszerű állandó kapcsolattartási pontokat és gyors kommunikációs csatornákat létrehozni a civil és katonai szervezetek között, valamint rendszeres, nem válsághelyzethez kötött szakmai egyeztetéseket tartani a kölcsönös megértés erősítése érdekében.

Jogi megfelelés és etikai szempontok integrálása[33]

A jogi és etikai keretek figyelmen kívül hagyása rövid távon gyorsabb reagálást eredményezhet, hosszú távon azonban aláássa az együttműködés legitimitását és a társadalmi bizalmat. A jogi bizonytalanság különösen válsághelyzetben bénító hatású lehet.

Javaslat: indokolt közös jogi és etikai iránymutatások kidolgozása, valamint célzott képzések szervezése annak érdekében, hogy a résztvevők pontosan tisztában legyenek jogosultságaikkal és kötelezettségeikkel a kiberkoordináció során. A gyakorlatok ezen a területen is lehetőséget biztosítanak a folyamatok szimulációjára, amennyiben nem egyértelműek a döntési pontok, akkor ezek finomhangolása még a konfliktusokat megelőzően lehetséges.

Szervezeti és stratégiai ajánlások

A nem egyértelmű felelősségi viszonyok és a hiányos incidenskezelési protokollok késleltetik a reagálást és növelik a szervezeti súrlódásokat. Ezzel szemben a tanuló szervezeti megközelítés hosszú távon növeli a rendszer ellenálló képességét.

Javaslat: szükséges a civil–katonai együttműködésben érintett szervezetek feladat- és hatáskörének egyértelmű rögzítése, valamint egy közös incidensértékelési és tapasztalatfeldolgozási mechanizmus bevezetése, amely biztosítja a folyamatos fejlődést. Célszerű a CIMIC-szakterület korábban kialakult feladatai kiterjesztésének vizsgálata a *kiberdomain* irányába,[34] a tapasztalatok átadása más civil szereplők részére is.

[33] Schmitt 2017.
[34] NATO CIMIC Centre of Excellence 2025a.

A kibertartalékos-rendszer kialakítása egyszerre képes növelni a nemzeti reziliencia szintjét, valamint racionalizálhatja a felhasznált erőforrásokat.

Összegzés

A tanulmányban a megfogalmazott célokkal összhangban azonosítottam a kibertér alapfogalmait és sajátosságait, végigkövettem a civil–katonai kapcsolatok alakulását annak érdekében, hogy kellő megalapozottsággal tudjak javaslatokat megfogalmazni a jövőbeni civil–katonai kibertérkapcsolatok koordinációjához. Vizsgálat alá vontam, hogy a CIMIC az információs műveletek részeként miként tud hatékonyan alkalmazkodni a kibertér követelményeihez a szakmai megújulás érdekében, hogyan tudja a jelenlegi és jövőbeni feladatrendszert racionalizálni és aktualizálni.

Összességében a civil–katonai kapcsolatok a kibertérben komplex, sokszereplős, adaptív hálózatként működnek. A CIMIC példája jól szemlélteti, hogyan lehet a koordinációt formálisan is támogatni, de az együttműködés teljes képe ennél jóval komplexebb, a siker kulcsa a folyamatos tanulás, a rugalmas szervezeti struktúra, a partnerség, a bizalom és a jogi megfelelés. Az evolúciós és tanulási folyamatok eredményeként folyamatosan új szerepkörök jelennek meg mind civil, mind katonai területen, ennek egyik látványos példája a kiberparancsnokok hálózata. Figyelemmel kísérve feladatrendszerük átalakulását, egyértelműen kijelenthető, hogy a katonai hálózatok felügyelete és irányítása mellett egyre hangsúlyosabb szerepet kap portfóliójukban a civil képességek időszakos irányítása a katonai művelet végrehajtásának érdekében. Ez merőben új szemléletet követel a katonai kibertérműveleti erők és a civil vállalati vezetők részéről is, meg kell találni az egészséges egyensúlyt és a közös nyelvet a feladat-végrehajtás során. A civil és katonai szereplőknek képesnek kell lenniük arra, hogy egységesen reagáljanak a kibervédelmi fenyegetésekre, miközben megőrzik autonómiájukat és alkalmazkodnak a gyorsan változó technológiai és társadalmi környezethez. Azok az országok, amelyek sikeresen integrálják a jogi kereteket, a képzéseket, a szimulációkat és a folyamatos tapasztalatcserét, hosszú távon fenntartható és hatékony civil–katonai kiberkoordinációt biztosíthatnak.

Jelenleg már több országban létezik kibertartalékos-rendszer, ahol IT- és kiberbiztonsági szakembereket vonnak be a nemzeti kiberbiztonság támogatására különösen háborús válság vagy komplex, több szektort érintő kibertámadás esetén. A rendszerek formája országonként eltérő, vannak formális tartalékos programok, önkéntes gyakorlatok, valamint különleges katonai vagy kormányzati egységek, amelyek tartalékos szakértelmet integrálnak. Ezen a területen jó példák léteznek, azonban uniformizált megoldások nem, minden nemzetnek a céljaihoz kapcsolódóan kell kialakítania az ideális koncepciót. Az ilyen jellegű kezdeményezések stratégiai elrettentő hatással is rendelkeznek, mert ebben az esetben az állam nyíltan jelzi, hogy nemcsak egy szűk, állandó kibererőre támaszkodik, hanem szükség esetén több száz vagy ezer, valós piaci tapasztalattal rendelkező szakembert (akár komplett, összeszokott céges csapatokat) tud mozgósítani; ebben az esetben a támadó fél számára megnő a bizonytalanság és a kockázat. Nem tudja előre, mekkora védelmi kapacitással, milyen gyors reagálással és milyen szakértelemmel fog szembesülni. A kibertartalékos-rendszer kialakítása

során a hatékonyság fokozása érdekében célszerű vizsgálni az információs műveletek teljes spektrumát, így adva új, korábban nem alkalmazott megoldási javaslatokat a szakterületi szakemberhiányból adódó problémákra.

A Magyar Honvédség a döntési folyamatok gyorsabbá és hatékonyabbá tételének érdekében a publikációban szereplő egységes alapelvek használatát már 2022. január 1-jén megkezdte a Kiber- és Információs Műveleti Központ megalakításával, amelynek feladatrendszere magába foglalja többek között a Magyar Honvédség kiberműveleti (CYBER OPS), civil–katonai együttműködési (CIMIC), lélektani műveleti (PSYOPS) és információskörnyezet-elemző (IEA) képességeinek biztosítását is. A publikációban szereplő javaslatok felhasználása lehetőséget biztosít a továbblépésre, azok tesztelését követően célszerű megkezdeni fokozatosan az integrációs folyamatot.

Felhasznált irodalom

2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről. Online: https://net.jogtar.hu/jogszabaly?docid=a2100140.tv

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

Balogh Péter (2025): Kibertérbeli műveletek 2016-ot követően – A kiberhadviselés mintázatai, trendjei, szereplői és kapcsolódásaik. *Hadtudomány,* 35(E-szám). Online: https://doi.org/10.17047/Hadtud.2025.35.E.1

Bencsik, András – Karpiuk, Mirosław (2023): The Legal Status of the Cyberarmy in Hungary and Poland. *Central European Journal of Social Sciences and Humanities,* 11(2), 19–31. Online: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_35467_cal_174696

Boeke, Sergei – Heinl, Caitríona – Veenendaal, Matthijs A. (2018): Civil-Military Relations & International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe. In Maybaum, M. – Osula, A.-M. – Lindström, L. (szerk.): *2015 7th International Conference on Cyber Conflict.* Tallinn: CCD COE. Online: https://doi.org/10.1109/CYCON.2015.7158469

Bonnyai Tünde – Kiss Adrienn – Tóth András szerk. (2023): *Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés. Kiber- és információbiztonsági tanulmányok.* Budapest: Ludovika. Online: https://doi.org/10.36250/01170_00

Clarke, Richard A. – Knake, Robert K. (2019): *The Fifth Domain.* New York: Penguin.

Deibert, Ronald J. (2003): Black Code: Censorship, Surveillance and the Militarization of Cyberspace. *Journal of International Studies,* 15(2), 33–56. Online: https://thesociologycenter.com/supscibiblog/BlackCode.pdf

Ertan, Amy et al. szerk. (2020): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn: CCD COE. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Haig Zsolt (2023): A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika, 41–60. Online: https://tudasportal.

uni-nke.hu/xmlui/handle/20.500.12944/102124?key=Kiberv%C3%A9delem%20%C3%A9s%20nemzetbiztons%C3%A1g%20kiss
Hunorfi, Péter – Farkas, Tibor (2025): Cybersecurity of Operational Technology in Critical Infrastructures. *Belügyi Szemle,* 73(1Ksz.), 183–197. Online: https://doi.org/10.38146/bsz-ajia.2025.v73.i1SI.pp183-197
Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148(5), 12–34. Online: https://doi.org/10.35926/HSZ.2020.5.1
Krasznay, Csaba (2024): Hacktivists, Proxy Groups, Cyber Volunteers. *Academic and Applied Research in Military and Public Management Science,* 23(3), 107–124. Online: https://doi.org/10.32565/aarms.2024.3.6
Krasznay, Csaba – Hámornik, Balázs Péter (2019): Human Factors Approach to Cybersecurity Teamwork – The Military Perspective. *Advances in Military Technology,* 14(2), 291–305. Online: https://doi.org/10.3849/aimt.01296
Kott, Alexander et al. (2018): Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153. *ArXiv.* Online: https://doi.org/10.48550/arXiv.1804.07651
NATO CIMIC Centre of Excellence (2025a): *CIMIC in the Cyberspace Domain: Fact Sheet*. Online: www.cimic-coe.org/wp-content/uploads/2025/03/20250303-uc-ccoe-factsheet-cyberspace-final.pdf
NATO CIMIC Centre of Excellence (2025b): *CIMIC Case Studies*. Online: www.cimic-coe.org/wp-content/uploads/2025/05/acaCIMICs_Case-Studies.pdf
NATO CIMIC Centre of Excellence (2025c): *CIMIC Handbook 2.1 NATO CIMIC*. Online: www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/ii-fundamentals/2-1-nato-cimic/
NATO Standardization Office (2020): *Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations.* Online: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
NATO Standardization Office (2025): *Standard AJP-3.19. Allied Joint Doctrine For Civil-Military Cooperation ED B V1.* Online: https://assets.publishing.service.gov.uk/media/685a8bdce9509f1a908eb108/AJP_3_19_EdB_CIMIC.pdf
NATO's Strategic Warfare Development Command (2025): *Strengthening Civil-Military Cooperation: The Role of NATO's Civil-Military Cooperation Centre of Excellence.* Online: www.act.nato.int/article/cimic-coe-2025/
Resperger István – Kiss Álmos Péter – Somkuti Bálint (2014): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest: Zrínyi.
Schmitt, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781316822524
Szádeczky, Tamás (2018): Cybersecurity Authorities and Related Policies in the EU and Hungary. *Central Eastern European eDem & eGov Days,* 331, 287–299. Online: https://doi.org/10.24989/ocg.v331.24
United Nations [é. n.]: *United Nations Charter.* Online: https://www.un.org/en/about-us/un-charter/full-text

VARGA Zsófi (2022): Civil-katonai együttműködés alkalmazása komplex hadműveleti környezetben. *Biztonságtudományi Szemle,* 4(1), 63–73. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/207/179

White House (2026): *President Trump's Cyber Strategy for America.* Online: www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

21. évfolyam (2026) 1. szám 77–92.
DOI: 10.32567/hm.2026.1.5

Répás József,[1] Berek László,[2] Oláh Norbert[3], Ujhegyi Péter,[4] Vinogradov Szergej[5]

Felsőoktatási hallgatók biztonságtudatossága a SAM-modell alapján[6]

Security Awareness among Higher Education Students Based on the SAM Model

Absztrakt

A digitális környezet gyors fejlődése és a kibertámadások növekvő száma a humán tényezőt a kiberbiztonság legsebezhetőbb elemévé tette. A felhasználók biztonságtudatosságának mérése ezért kulcsfontosságú a hatékony védelem és a célzott oktatási programok kialakítása szempontjából. Jelen kutatás a Security Awareness Model (Biztonságtudatossági Modell, SAM) bemutatására és empirikus tesztelésére vállalkozik, amely a korábbi Human Aspects of Information Security Questionnaire (HAIS-Q) modellt továbbfejlesztve a tudás–attitűd–viselkedés dimenziókat tíz szakmai terület mentén – többek között jelszóhasználat, webes biztonság, személyes adatok védelme vagy incidensmenedzsment – integrálja. A 2025 tavaszán végzett pilotkutatás 132 felsőoktatási hallgató válaszain alapult, és célja a modell konstrukcióinak megbízhatósági és érvényességi vizsgálata volt. Az eredmények alapján mindhárom komponens dimenziói szignifikánsan hozzájárulnak az általános biztonsági tudáshoz, ugyanakkor néhány tétel újrafogalmazása indokolt a mérési pontosság javítása

[1] Gábor Dénes Egyetem, e-mail: repas.jozsef@alverad.hu
[2] Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola, e-mail: berek.laszlo@uni-obuda.hu
[3] Debreceni Egyetem Informatikai Kar Adattudomány és Vizualizáció Tanszék, e-mail: olah.norbert@inf.unideb.hu
[4] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: ujhegyi.peter@uni-obuda.hu
[5] Budapesti Metropolitan Egyetem, Módszertan Intézet, e-mail: szvinogradov@metropolitan.hu
[6] A cikk a TKP2021-NVA-05 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP 2021 pályázati program finanszírozásában valósult meg.

érdekében. A hallgatók a legnagyobb egyetértést a klasszikus biztonsági kockázatok (például ismeretlen USB-eszközök, adathalászat) terén mutatták, míg a szabályozási tudatosság és az új technológiákhoz kapcsolódó attitűdök esetében jelentős bizonytalanság tapasztalható. A SAM-modell alkalmas az információbiztonsági tudatosság komplex, többdimenziós feltárására, és alapot nyújt nagymintás, országos vizsgálatokhoz, amelyek hozzájárulhatnak a biztonsági kultúra fejlesztéséhez a felsőoktatásban és a társadalom szélesebb körében.

Kulcsszavak: információbiztonság, biztonságtudatosság, SAM-modell, HAIS-Q, felsőoktatás, pilotkutatás

Abstract

The rapid development of the digital environment and the increasing number of cyberattacks have made the human factor the most vulnerable element of cybersecurity. Measuring users' security awareness is crucial for adequate protection and developing targeted education programmes. This research aims to present and empirically test the Security Awareness Model (SAM), which builds on the previous HAIS-Q model by integrating the Knowledge–Attitude–Behaviour dimensions across ten professional areas, including password use, web security, personal data protection, and incident management. The pilot study, conducted in the spring of 2025, was based on the responses of 132 higher education students and aimed to test the reliability and validity of the model's constructs. Based on the results, all three component dimensions contribute significantly to general security knowledge, but some items need to be reworded to improve measurement accuracy. The students agreed on classic security risks (e.g., unknown USB devices, phishing). At the same time, there was significant uncertainty in regulatory awareness and attitudes toward new technologies. The SAM model is suitable for the complex, multidimensional exploration of information security awareness and provides a basis for large-scale, nationwide studies that can contribute to developing a security culture in higher education and society.

Keywords: information security, security awareness, SAM model, HAIS-Q, pilot research, higher education

Bevezetés

Az információbiztonság napjaink egyik kiemelt területe, mivel a technológia rohamos fejlődésével párhuzamosan a kibertámadások egyre gyakoribbak és súlyos pénzügyi, reputációs, sőt érzelmi károkat okozhatnak az érintett szervezeteknek és felhasználóknak.[7] Az információbiztonság tág értelemben magában foglalja mind a digitális, mind a nem digitális formában kezelt információk védelmét, míg a kiberbiztonság ennek azon részterületét jelenti, amely kifejezetten a hálózati és online környezetben megjelenő fenyegetésekre és védelmi mechanizmusokra fókuszál. A digitális társadalomban az információbiztonság szerepe felértékelődött, hiszen a technológiai

[7] Ahlan–Lubis–Lubis 2015.

védelem hatékonyságát egyre inkább az emberi tényező határozza meg. A mesterséges intelligencia, a felhőszolgáltatások, az online tanulási környezetek és az okoseszközök elterjedése soha nem látott mértékben tágította a digitális ökoszisztéma határait, miközben a kiberfenyegetések száma és komplexitása is rohamosan nő.

A nemzetközi szakirodalom egyre inkább rámutat arra, hogy a technológiai fejlesztések önmagukban nem elegendőek a kockázatok csökkentésére: a biztonságos működés kulcsa az információbiztonsági tudatosság fejlesztése és mérése. Az információbiztonsági tudatosság olyan komplex kompetencia, amely magában foglalja a biztonsági ismeretek meglétét, a fenyegetések felismerését, az azokhoz való attitűdöt, valamint a biztonságos viselkedés gyakorlati megvalósítását. A digitális korszakban az egyének – különösen a felsőoktatási hallgatók – nem csupán információfogyasztók, hanem aktív tartalom-előállítók és hálózati szereplők, akik döntéseikkel közvetlenül befolyásolják az egyetemi és intézményi vagy céges biztonsági környezet stabilitását.

Számos kutatás igazolja, hogy a biztonságtudatos viselkedés hiánya közvetlenül növeli az adatszivárgások, az adathalász-támadások és a jogosulatlan hozzáférések kockázatát.[8] Mindez különösen releváns a felsőoktatásban, ahol a digitális transzformáció, a távoktatás és az online kollaborációs platformok mindennapos használata új biztonsági kihívásokat teremt. A hallgatók nagy része a fiatal felnőtt korosztályba tartozik, akik magas technológiai jártassággal, de gyakran alacsony biztonsági tudatossággal rendelkeznek. Ennek következtében a felsőoktatási intézmények számára az információbiztonsági kultúra fejlesztése nem csupán technikai, hanem stratégiai oktatáspolitikai feladat is.

Ebben a kontextusban válik relevánssá a biztonságtudatosság mérésének modernizálása, olyan eszközökkel, amelyek képesek a felhasználók tudását, attitűdjeit és viselkedését egyaránt feltárni, és figyelembe veszik a környezeti, kulturális és intézményi hatásokat is. A SAM-modell ezen elvek mentén épül fel, és célja, hogy átfogóbb és korszerűbb képet adjon a felhasználók biztonságtudatossági szintjéről.[9]

Ebben a dinamikusan változó környezetben az információbiztonsági tudatosság kiemelt, mivel a humán tényező gyakran a leggyengébb láncszem, így a felhasználók biztonságtudatosságának szintje döntően befolyásolja a szervezetek és egyének védettségét. A biztonságtudatosság méréséhez hatékony módszerekre van szükség, hiszen csak így azonosíthatók a gyenge pontok és alakíthatók ki célzott védelmi stratégiák.

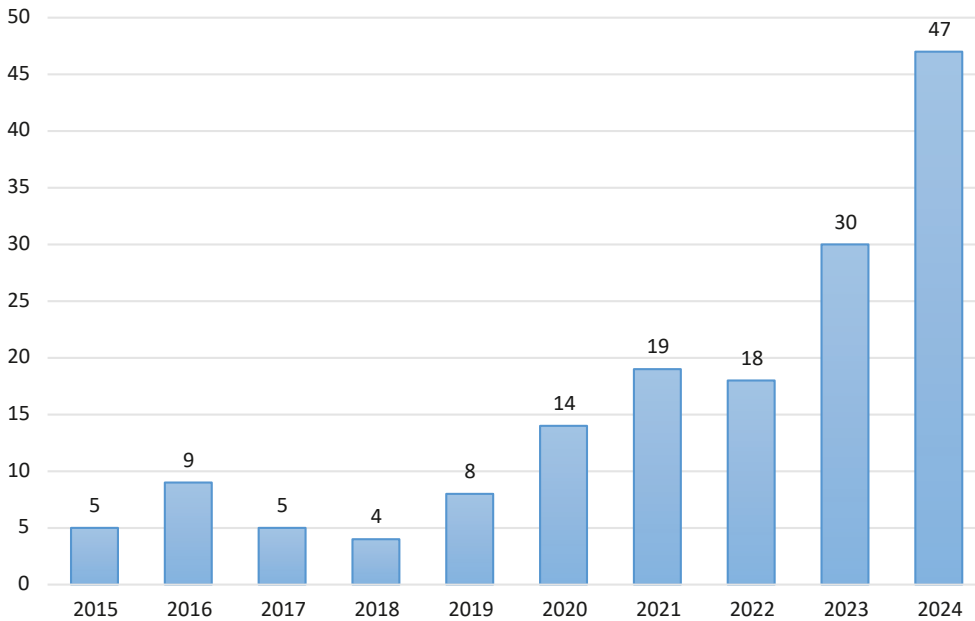
Tudományos megközelítés és a kapcsolódó modell

Az információbiztonsági tudatossági szint mérése hangsúlyos volt mind nemzetközi, mind hazai vonatkozásban az elmúlt évtizedekben. A témában megjelent kutatási eredmények, publikációk feltérképezését a Scopus adatbázis felületén végeztük el. A keresőkifejezésben kifejezetten a felsőoktatási környezetben végzett, az információbiztonsági tudatosságra irányuló felmérésekre voltunk kíváncsiak. A Scopusban alkalmazott, konkrét keresőkifejezésünk a következő volt:

[8] Parsons et al. 2017; Hong–Furnell 2021.
[9] Répás et al. 2024.

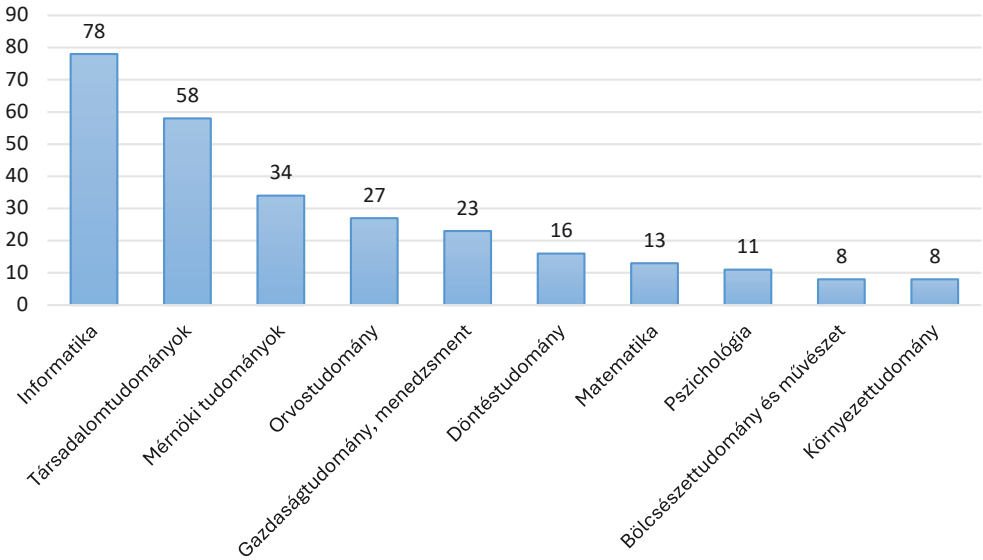
TITLE-ABS-KEY („information security" OR „cybersecurity" OR „data protection" OR „infosec") AND TITLE-ABS-KEY („awareness" OR „understanding") AND TITLE-ABS-KEY („survey" OR „questionn*") AND TITLE-ABS-KEY („higher education" OR „universit*" OR „college" OR „students") AND PUBYEAR > 2014 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"re")) AND (LIMIT-TO (LANGUAGE,"English"))

A kapott eredmény egyértelműen mutatja, hogy a témával kapcsolatos kutatások száma évről évre nő. Természetesen a tudományos kutatások színterei leginkább az egyetemek, felsőoktatási intézmények, így kézenfekvő, hogy hasonló felmérések a legegyszerűbben, leggyorsabban az egyetemi hallgatók bevonásával végezhetők el (1. ábra).



1. ábra: Kapcsolódó publikációk száma, 2015–2024, Scopus
Forrás: a szerzők szerkesztése

A publikációk szakterületi eloszlás szerinti vizsgálata igazolja, hogy a vizsgált terület multidiszciplináris megközelítésben is értelmezhető. A vizsgált folyóiratcikkek a legkülönbözőbb *subject area* besorolásba tartozó folyóiratokban jelentek meg. A 2. ábra a top 10 szakterületet mutatja be. Ebben is látható, hogy – természetesen – az informatika besorolású folyóiratok állnak az első helyen, de rögtön mögötte már a társadalomtudomány áll, sőt az üzleti tudományok is bekerült az első 5 közé.



2. ábra: Publikációk szakterület szerint, Scopus/Scimago
Forrás: a szerzők szerkesztése

A találatok közül a legtöbb citációval rendelkező 20 publikáció áttekintésével a méréshez használt eszközökről, a viselkedést befolyásoló fő tényezőkről, illetve a kutatások ajánlásairól is képet kaptunk.

A kutatások módszertani szempontból túlnyomórészt kvantitatív kérdőíves felmérésekre épültek,[10] kisebb részben vegyes módszertanú vizsgálatokra,[11] amelyek interjúkkal és fókuszcsoportokkal mélyítették el a hallgatói attitűdök megértését. A mérési keretek közül a legelterjedtebb a HAIS-Q – amely a tudás *(knowledge),* attitűd *(attitude)* és viselkedés *(behaviour)* összefüggéseit vizsgálja[12] –, valamint a tervezett viselkedés elmélete (*theory of planned behaviour,* TPB), amely az attitűd, a szubjektív norma és az észlelt viselkedéses kontroll kapcsolatát modellezi.[13]

A kutatások eredményei alapján az információbiztonsági viselkedést több, egymással összefüggő tényező befolyásolja. Az oktatási háttér és a szakterület fontos szerepet játszik: az informatikai és mérnöki képzéseken tanuló hallgatók információbiztonsági tudatossága és ismeretszintje szignifikánsan magasabb, mint más szakterületek hallgatóié. Ezt a különbséget részben a technikai ismeretek mélysége, részben pedig az adott képzési területeken nagyobb hangsúlyt kapó adatvédelem és információbiztonsági oktatás magyarázza.

A demográfiai tényezők szintén hatással vannak a tudatosságra: a férfi hallgatók és a városi környezetben tanulók jellemzően magasabb információbiztonsági

[10] Alqahtani 2022; Taha–Dahabiyeh 2021.
[11] Módné Takács – Pogátsnik 2024; Blažič–Blažič 2022.
[12] Parsons et al. 2017.
[13] Alanazi–Freeman–Tootell 2022.

tudatosságot mutatnak, mint női és vidéki társaik.[14] Ezek a különbségek arra utalnak, hogy a társadalmi és környezeti háttér is alakítja az információbiztonsággal kapcsolatos attitűdöket és viselkedést.

A személyiségvonások vizsgálata további fontos összefüggéseket tárt fel. A lelkiismeretesség, a barátságosság és a nyitottság pozitív kapcsolatban áll a biztonságosabb online viselkedéssel, ami azt jelenti, hogy az egyéni pszichológiai jellemzők befolyásolják, mennyire hajlamos valaki a biztonsági szabályok betartására és a kockázatok tudatos kezelésére.[15] A személyiség tehát meghatározó pszichológiai prediktornak tekinthető a biztonságtudatos magatartás kialakulásában.

Ezzel párhuzamosan az intézményi és helyzeti támogatásnak is jelentősége van. Az eredmények szerint a megfelelő intézményi háttér, a támogató környezet és a korábbi tréningek egyaránt javítják a hallgatók információbiztonsági tudatosságát.[16] A kutatások hangsúlyozzák, hogy a biztonsági magatartás nemcsak az egyéni döntésektől, hanem a felsőoktatási intézmény szervezeti kultúrájától is függ: a példamutató oktatói gyakorlat, az elérhető támogató infrastruktúra és a rendszeres képzések mind növelik a biztonságos viselkedés valószínűségét.

Végül az attitűdök és a viselkedési szándék is lényeges tényezőknek bizonyultak. Az attitűdök, a szubjektív normák és az észlelt viselkedéses kontroll – a TPB alapján – kimutathatóan befolyásolják a biztonságos viselkedésre irányuló szándékot.[17] Ugyanakkor a tényleges viselkedés gyakran csak részben követi a szándékot, ami rávilágít arra, hogy a szokások és a környezeti támogatás nélkülözhetetlenek ahhoz, hogy a tudás és a szándék ténylegesen biztonságtudatos cselekvéssé alakuljon.

A korábbi mérési megközelítések közül a legismertebb a HAIS-Q, amely a KAB-keretet alkalmazva vizsgálta a felhasználók biztonsági ismereteit, hozzáállását és viselkedését.[18] Bár a HAIS-Q széles körben használt és megbízható eszköz, a gyorsan változó technológiai és szabályozási környezetben több hiányosság is felszínre került. A klasszikus kérdőív ugyanis nem tudta teljes mértékben lefedni azokat a modern kihívásokat, amelyeket a felhőalapú szolgáltatások, a többfaktoros hitelesítés, a kollaborációs platformok vagy éppen a GDPR- és a NIS2-szabályozások teremtettek. Ezen hiányosságok kiküszöbölésére született meg a SAM-modell, amely a HAIS-Q alapjaira épít, ugyanakkor jelentősen modernizálja és kibővíti azt.

SAM-modell

A biztonságtudatosság mérésének szükségességét korábban a HAIS-Q-modell alapozta meg, amely a KAB-keretet használta a felhasználói biztonsági magatartás vizsgálatára. Ez a struktúra lehetővé teszi, hogy ne csak az ismeretek szintjét, hanem a belső motivációkat és a tényleges cselekvési mintákat is feltárjuk. Ugyanakkor a digitális környezet átalakulása (felhő, kollaborációs platformok, MFA, AI, szabályozások) indokolttá tette

[14] Hong–Furnell 2021; Aljohni et al. 2021.
[15] Shappie–Dawson–Debb 2020.
[16] Répás et al. 2024; Alharbi–Tassaddiq 2022; Al-Janabi – Al-Shourbaji 2016.
[17] Alanazi–Freeman–Tootell 2022.
[18] Parsons et al. 2017; Parsons et al. 2014; Parsons et al. 2013; McCormac et al. 2017.

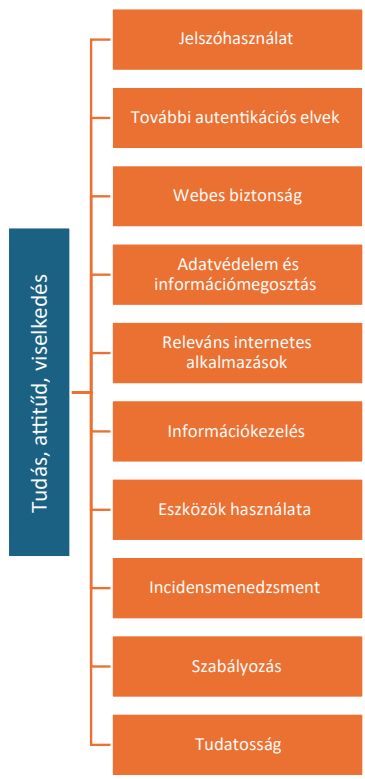
a modell kiterjesztését. A SAM ezért a HAIS-Q modernizált, kibővített változatának tekinthető, amely a kontingenciaelmélet szellemében alkalmazkodik a környezeti és technológiai változásokhoz. A SAM struktúrája alapvetően a tudás–attitűd–viselkedés (TAV) logikára épül. A modellben minden dimenziót három aspektusból vizsgálunk: egyrészt azt mérjük, hogy a válaszadók milyen ismeretekkel rendelkeznek az adott területen, másrészt feltárjuk a biztonsághoz kapcsolódó attitűdjeiket, végül pedig a tényleges cselekvéseket és viselkedési mintákat is rögzítjük. Ez a megközelítés lehetővé teszi, hogy ne csupán a tudás meglétét, hanem annak attitűdökön keresztüli átfordulását és gyakorlati alkalmazását is vizsgáljuk.[19]

A modell tíz szakmai dimenzió mentén közelíti meg a biztonságtudatosság mérését, amelyet a 3. ábra mutat be, és a kérdőívben szereplő tételek ezekre a dimenziókra épülnek. A többdimenziós szakmai felépítés jelentősége abban rejlik, hogy lehetővé teszi a biztonságtudatosság komplex, rendszerszintű értelmezését, azaz nem csupán az elszigetelt ismeretek meglétét vizsgálja, hanem feltárja az egyes szakmai területek közötti különbségeket és hiányosságokat is. A modell így alkalmas a kritikus tudáshiányok, a kockázatos attitűdök és a fejlesztést igénylő viselkedési minták azonosítására, valamint megalapozza a célzott, dimenzióspecifikus tudatosítási beavatkozások tervezését. A jelszóhasználat dimenziója a jelszavak létrehozásának, kezelésének és frissítésének gyakorlatát vizsgálja, valamint feltárja a jelszóválasztással kapcsolatos tipikus hibákat. A további autentikációs elvek dimenziója a modern hitelesítési gyakorlatokra koncentrál, különös tekintettel a többfaktoros hitelesítésre (MFA), amelyekre napjainkban példa az SMS-ben vagy mobilalkalmazásban kapott kódok és a biometrikus azonosítás alkalmazása. A webes biztonság dimenziója az internetböngészés során jelentkező fenyegetések kezelését vizsgálja, beleértve az adathalász-támadások felismerését, a biztonságos weboldalak (HTTPS) használatát és a gyanús letöltések elkerülését. A *privacy* és információmegosztás a személyes adatok és információk tudatos kezelésére irányul, különösen a közösségimédia-használat során.

Az internetszolgáltatások használata a felhőalapú platformok, az e-mail-rendszerek és a kollaborációs eszközök biztonságos használatát értékeli, hangsúlyozva a jogosultságkezelés és az adatmegosztás biztonsági kérdéseit. Az információkezelés a bizalmasság, integritás és rendelkezésre állás elveinek megvalósulását méri, kitérve az adattárolási, adatkezelési és titkosítási gyakorlatokra. Az eszközhasználat dimenziója a digitális eszközök védelmét vizsgálja, különös figyelmet fordítva a frissítések rendszeres elvégzésére, a vírusirtó és tűzfal használatára, valamint a saját eszközök munkahelyi használatának (*bring your own device,* BYOD – „hozd a saját eszközödet") biztonsági vonatkozásaira. Az incidensmenedzsment-dimenzió azt méri, hogy a válaszadók képesek-e felismerni a gyanús eseményeket, tudják-e, hogyan kell azokat jelenteni, és mennyire ismerik az incidensek kezelésére vonatkozó eljárásokat. A szabályozás dimenziója a kiberbiztonsági és adatvédelmi szabályok – különösen a GDPR és a NIS2 – ismeretét és gyakorlati alkalmazását vizsgálja. Végül a tudatosság dimenziója az általános biztonsági kultúrára és a humán tényezőkre fókuszál, mérve a kockázatészlelés szintjét és a tudatos magatartás jelenlétét, amelyet gyakran a *human firewall* koncepcióval írnak le.

[19] Répás et al. 2024; Bak et al. 2024; Berek et al. 2024; Répás et al. 2025.

A SAM újdonsága több dimenzióban is megnyilvánul. Elsőként: a modell holisztikus szemléletet képvisel, mivel nem csupán a technikai ismeretek szintjére korlátozódik, hanem a jogszabályi megfelelést, a felhasználói attitűdöket és a szervezeti kultúra szempontjait is integrálja. A SAM nemcsak az egyéni tudatosságot, hanem a tágabb társadalmi és intézményi környezethez való alkalmazkodást is képes így értékelni. Másodsorban a modell naprakészen követi a digitális környezet kihívásait, hiszen beépíti azokat a területeket, amelyek a legújabb technológiai trendekből fakadóan váltak fontossá. Ilyen például a felhőalapú szolgáltatások biztonsága, a mesterséges intelligencia által támogatott rendszerek használatának kockázatai, az IoT-eszközök elterjedése vagy a távmunkához kapcsolódóan megjelenő biztonsági kockázatok, amelyek új típusú sebezhetőségeket és adatvédelmi problémákat hoztak magukkal. Harmadrészt a SAM rugalmas és adaptív keretrendszert kínál, amely a kontingenciaelmélet alapján különböző szervezeti és társadalmi környezetekhez is illeszkedik, ezáltal nem statikus mérőeszközként, hanem folyamatosan fejleszthető modellként működik. Végül a SAM a KAB (tudás–attitűd–viselkedés) keretet magasabb szintre emeli: nem elszigetelt komponensekként kezeli a három tényezőt, hanem dinamikus kölcsönhatásban vizsgálja őket. Ez a komplexitás teszi lehetővé, hogy a SAM pontosabb, mélyebb és a gyakorlati kontextusban is jobban értelmezhető eredményeket adjon, mint a korábbi modellek.



3. ábra: A kutatás elméleti modellje
Forrás: a szerzők szerkesztése ***Répás*** *et al. 2024 alapján*

Eredmények

A 2025 tavaszán lebonyolított pilot-adatfelvétel célja az volt, hogy a felsőoktatási hallgatók körében tesztelje az információbiztonsági tudatosság mérésére szolgáló kérdőívet. A vizsgálat fókusza az elemek érthetőségének, megkülönböztető erejének és a válaszmegoszlások jellegzetességeinek feltárása volt, mielőtt a nagymintás, országos adatfelvétel megkezdődne. Az adattisztítás eredményeként a minta összesen 132 fő hallgatót foglalt magában, amely nagyságrendileg elegendő arra, hogy a kérdőív megbízhatóságát és belső logikáját ellenőrizze. Az adatfelvétel célja a kérdőív tételeinek kipróbálása és a statisztikai jellemzők feltárása volt. Az állításokat a válaszadók 1–6 fokozatú Likert-skálán értékelték (1 = egyáltalán nem ért egyet, 6 = teljes mértékben egyetért), külön „Nem tudom" opció nem volt.

A felsőoktatási hallgatói pilotminta főbb jellemzői

A minta szinte teljes egészében a fiatal felnőttek korcsoportját képviseli. A válaszadók többsége 19 és 22 év közötti: a 20 évesek (31,8%) és a 21 évesek (28,8%) adják a legnagyobb arányt. Az idősebb hallgatók (23–27 évesek) aránya alacsony (összesen ~ 6%), míg a 30 év feletti korosztály csak szórványosan fordul elő. Ez a megoszlás jól tükrözi a nappali tagozatos alapképzésben részt vevő hallgatók életkori szerkezetét, ugyanakkor a felsőoktatás teljes hallgatói populációjához képest alulreprezentált a mesterszakos (23 év feletti) korosztály. A nemek szerinti eloszlás jelentős férfitöbbséget mutat: a válaszadók 79,5%-a férfi, 18,2%-a nő, míg 2,3% nem adott választ. Ez eltér az országos felsőoktatási tendenciáktól, ahol jellemzően enyhe női többség figyelhető meg. A minta tehát az életkor tekintetében közelíti, a nemek arányában viszont eltéríti a felsőoktatási hallgatói populáció szerkezetét. A válaszadók döntő része városi környezetben él. A legnagyobb arányban megyei jogú városból érkeztek (36,4%), őket az „egyéb városok" követik (31,8%). A községekben vagy falvakban élők aránya 25,0%, míg a fővárosból mindössze 3,8% került a mintába. A mintát erősen dominálja az Észak-Alföld régió (73,5%), amely összefügg a mintavétel debreceni központjával. A többi régió marginális arányban szerepel: Észak-Magyarország (6,1%), Dél-Alföld (3,0%), valamint a dunántúli régiók, Pest és Budapest egyenként 2–3%-os arányban jelennek meg. Így az adatfelvétel nem országos lefedettséget, hanem inkább regionális próbavizsgálatot biztosított. A minta szerkezeti jellemzői közvetlenül hatással vannak az eredmények értelmezésére is. A fiatal, döntően alapképzésben tanuló hallgatók digitális környezete és tapasztalati háttere magyarázza, hogy bizonyos kérdéskörökben határozott válaszokat adtak, más területeken viszont inkább bizonytalanságot jeleztek.

A biztonságtudatosság mintázatai a hallgatói pilotmintában

Azokban az esetekben merülhet fel bizonytalanság, ha a válaszadók jelentős része a skála középső értékeit (3 vagy 4) választja. A felmérés eredményei szerint néhány

szakmai kérdésnél a középértékválaszok aránya meghaladta az 50%-ot, ami a hallgatók bizonytalanságát vagy kialakulatlan attitűdjeit tükrözi. Ezek a témakörök a szabályozási kérdések és az új technológiák, amelyek terén a hallgatók válaszaiban bizonytalanság mutatkozott meg, például az előírások és szabályok ismeretét mérő tételnél (átlag: 3,41; szórás: 1,01). Ezzel szemben a klasszikus információbiztonsági helyzetekben határozott konszenzus figyelhető meg. A legnagyobb egyetértést az a kijelentés váltotta ki, hogy a hallgatók nem csatlakoztatnának nyilvános helyen talált USB-pendrive-ot a számítógépükhöz (átlag: 5,61; szórás: 0,70). Magas értéket kapott továbbá az a megállapítás is, hogy a mesterségesintelligencia-alapú alkalmazások adatbiztonsági kockázatokat hordoznak (átlag: 5,36; szórás: 0,77). Ezzel szemben a legkisebb egyetértést olyan állítások váltották ki, amelyek a felhasználói tudatosság és a képzés szerepéhez, illetve a technológiai környezet biztonságának megítéléséhez kapcsolódnak. A hallgatók körében alacsony volt a támogatottsága annak, hogy mindig átnéznék a használati feltételeket és szabályzatokat (átlag: 2,84), vagy hogy az információbiztonsági képzések érdemben segítenének az online veszélyek felismerésében (átlag: 2,78). Gyenge egyetértés mutatkozott a törölt adatok visszaállíthatóságának problémáját (átlag: 2,74) és különösen a felhőben tárolt adatok biztonságának kérdését illetően (átlag: 1,92). Mindez arra utal, hogy míg a hallgatók a klasszikus biztonsági kockázatokat egyértelműen felismerik, addig a szabályozási tudatosság, a képzések hatékonysága és az új technológiákhoz kapcsolódó attitűdök terén nagy fokú bizonytalanság és széttartás tapasztalható.

Az itemek többségénél a szórás alacsony vagy közepes szintet mutatott, ami a válaszadók közötti konszenzus jele. Ugyanakkor néhány állításnál szokatlanul magas szórás jelentkezett, ami a hallgatói közösség megosztottságát tükrözi. Ilyen például az a kijelentés, miszerint a bizalmas adatokat tartalmazó nyomtatványok ugyanolyan módon megsemmisíthetők, mint azok, amelyek nem tartalmaznak bizalmas adatokat (szórás: 1,61). Ez jól jelzi, hogy a hallgatók egy része tisztában van az iratmegsemmisítés sajátos biztonsági követelményeivel, míg mások ezt nem tekintik lényeges különbségnek. Hasonlóképpen magas szórás mutatkozott a törölt adatok visszaállíthatóságáról szóló tételnél (szórás: 1,59), ami arra utal, hogy a válaszadók eltérően ítélték meg az adattörlés és a formázás biztonsági kockázatát. A legnagyobb megosztottság azonban a jelszavak böngészőben való tárolásának megítélésében mutatkozott („Az eszközeim böngészőjében nem mentem el a jelszavaimat", szórás: 1,69). E tétel esetében világosan elkülönültek azok, akik biztonsági kockázatként értékelik a böngészőben mentett jelszavakat, és azok, akik a kényelmi szempontokat előtérbe helyezve elfogadják ezt a gyakorlatot. Ezek a magas szórású tételek különösen fontosak a pedagógiai beavatkozások szempontjából, mivel rámutatnak azokra a területekre, ahol a tudatosítás és az egységes minimumszint kialakítása a hallgatói közösségben elengedhetetlen.

A tudás modellelem empirikus érvényessége

Jelen fejezetben az információbiztonsági tudatosság mérésére kidolgozott SAM-modell tudás komponensének empirikus érvényességét vizsgáljuk. A teljes modell három fő komponensből épül fel, azonban a cikkben a tudás dimenziót mutatjuk be részletesen és teszteljük statisztikailag. A tudás komponenst a SAM elméleti keretrendszerének megfelelően hierarchikus, két szintből álló formatív mérési struktúrában operacionalizáltuk, amelynek empirikus vizsgálatát a következő alfejezetekben mutatjuk be. A hierarchikus felépítés lehetővé teszi, hogy az egyes szakmai dimenziók külön-külön is értelmezhetők legyenek, miközben együttesen alkotják az általános információbiztonsági tudás konstrukcióját.

Elsődleges formatív szint (indikátorok → dimenziók)

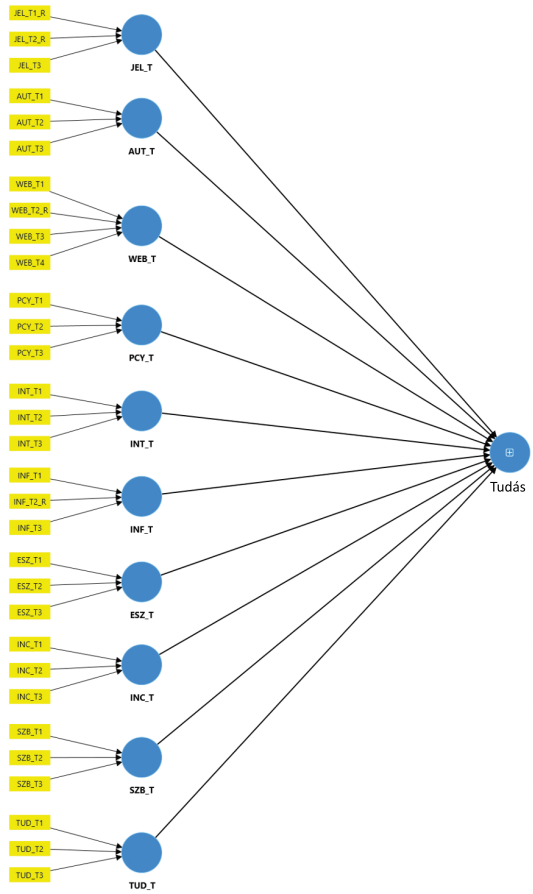
Az információbiztonsági tudást tíz különálló dimenzió mentén ragadtuk meg. Ezek a dimenziók a jelszóhasználathoz, az autentikációhoz, a webes biztonsághoz, az adatvédelemhez és információmegosztáshoz, a releváns internetes alkalmazások használatához, az információkezeléshez, az eszközhasználathoz, az incidensmenedzsmenthez, a szabályozási ismeretekhez, valamint az általános tudatossághoz kapcsolódnak (JEL_T, AUT_T, WEB_T, PCY_T, INT_T, INF_T, ESZ_T, INC_T, SZB_T, TUD_T). Minden dimenziót három, Likert-skálán mért állítás reprezentált, amelyek az adott tudásterület különböző aspektusait ragadták meg. Az indikátorok formatív módon járultak hozzá az adott dimenzió kialakításához, vagyis a dimenzió értékét nem tükrözték, hanem annak konstitutív elemeiként építették fel a konstrukciót.

Másodlagos formatív szint (dimenziók → tudás)

Az általános „tudás" konstrukciót a tíz dimenzió kompozit módon alkotja meg, amelyeket a 4. ábra szemléltet. Az egyes dimenziók nem feltétlenül korrelálnak egymással, de együtt képezik a biztonságtudatos gondolkodás alapját. Így az „általános tudás" nem egy egységes, homogén képesség, hanem több, egymást kiegészítő terület eredője.

Az adattisztítás eredményeként kapott adatállományból került sor a tudás komponens elméleti modelljének empirikus érvényességi vizsgálatára, a SmartPLS 4 szoftver[20] alkalmazásával, PLS-alapú strukturális egyenletmodellezés (PLS-SEM) módszerével.

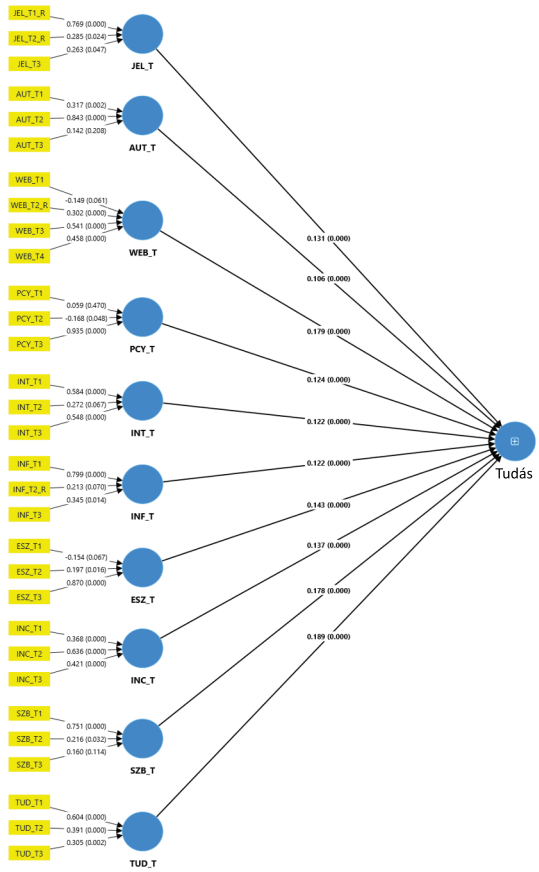
[20] A SmartPLS 4 egy grafikus felülettel rendelkező PLS-SEM (partial least squares structural equation modeling) szoftver, amely látens változós mérési és strukturális modellek elemzésére szolgál.



4. ábra: A tudás modellelem hierarchikus felépítése
Forrás: a szerzők szerkesztése

Az „R" jelölés az indikátorok (állítások) kódjában azt jelöli, hogy az adott állítás ellentétes tartalmú a dimenzió többi tételéhez képest, így a tudás konstruktum megfelelő mérhetősége érdekében inverz módon került be a modellbe. A tudás modellelem empirikus vizsgálata (5. ábra) eredményeként megállapítható, hogy a modell minden dimenziója szignifikáns súllyal járul hozzá az általános „tudás" konstrukcióhoz (minden út együttható esetében: $p < 0{,}001$), ami azt jelenti, hogy a dimenziók empirikusan megalapozottan képezik az általános tudáskomponenst.

Ugyanakkor néhány indikátor (például PCY_T1, WEB_T1, AUT_T3) alacsony vagy nem szignifikáns hozzájárulást mutatott a saját dimenziójához, ami a mérési modell finomításának szükségességére hívja fel a figyelmet.



5. ábra: A tudásmodell és annak aldimenziói empirikus érvényessége
Forrás: a szerzők szerkesztése

A tudás – adatvédelem és információmegosztás szakterületen például a PCY_T1 állítás („Privát böngésző használatakor a böngészési előzmények nem tárolódnak, de tevékenységünk nincs titkosítva") nem járult hozzá szignifikánsan a konstrukció méréséhez (β = 0,059; p = 0,470), míg a PCY_T2 tétel („Nem minden információ tehető közzé bármilyen weboldalon, még akkor sem, ha az a feladataim elvégzését segítené") negatív súlyt mutatott (β = –0,168; p = 0,048), ami fogalmi vagy értelmezési problémára utalhat. Hasonló jelenségek más dimenziókban is megfigyelhetők. Az autentikáció területen az AUT_T3 indikátor (β = 0,142; p = 0,208) nem mutatott szignifikáns kapcsolatot a mögöttes konstrukcióval, ami arra utal, hogy a tétel tartalma nem illeszkedik kellő pontossággal a mérni kívánt fogalomhoz. A webes biztonság esetében a WEB_T1 állítás (β = –0,149; p = 0,061) egyszerre gyenge (nem

szignifikáns) és inverz (negatív irányú) kapcsolatot jelez, ami a tétel újrafogalmazásának és tartalmi érvényességének újragondolását indokolja. Ezek az eredmények nem gyengítik a modell általános érvényességét, ugyanakkor rámutatnak arra, hogy a jövőbeni adatgyűjtések és modellépítések során érdemes lehet a mérési állításokat finomítani, pontosítani és a kulturális-nyelvi kontextushoz igazítani a megbízhatóság további növelése érdekében. Mindezek arra utalnak, hogy bizonyos állítások esetében nem csupán a statisztikai szignifikancia hiánya, hanem az értelmezési kontextus, a nyelvi megfogalmazás és a kulturális sajátosságok is befolyásolhatják a mérés megbízhatóságát. A jövőbeli adatgyűjtések és modellépítések során ezért indokolt ezen tételek átfogó tartalmi és módszertani felülvizsgálata, illetve szükség esetén új, pontosabban operacionalizált mérési állítások kidolgozása. Összességében a modell alkalmas az információbiztonsági tudás komplex, többdimenziós mérésére.

Jövőbeli tervek

A hallgatói adatokon végzett pilotkutatás eredményei megteremtik az alapot a kutatási és fejlesztési lépések következő szakaszához, amelyek végső célja a biztonságtudatosság átfogóbb vizsgálata és gyakorlati erősítése, amelyhez a közeljövőben nagymintás adatfelvételek indulnának mind a lakosság, mind a vállalati szféra körében. A lakossági vizsgálatok lehetőséget adnak arra, hogy feltárjuk a társadalom különböző csoportjai közötti tudás- és attitűdbeli eltéréseket, míg a vállalati minták elemzése rávilágít a szervezeti kultúra erősségeire, valamint azokra a hiányosságokra, amelyek fokozott kockázatot jelenthetnek. Az adatfelvételt részletes statisztikai elemzések és összehasonlító vizsgálatok követik, amelyek azonosítani tudják majd a kritikus tudáshiányokat, a kockázatos attitűdöket és a fejlesztést igénylő viselkedésmintákat.

A kutatás nem csupán diagnosztikai célokat szolgál, hanem közvetlen fejlesztési és felhasználási lehetőségeket is nyújtana. Az eredmények alapján célzott oktatási és biztonságtudatossági programok készülhetnek, amelyek magukban foglalhatják az iskolai és felsőoktatási tananyagok bővítését, felnőttképzési modulok kialakítását, valamint a vállalatokra szabott tréningek és belső szabályozási ajánlások kidolgozását. Emellett szektor- és régióspecifikus programokhoz, valamint széles körű tudatosító kampányokhoz nyújthat segítséget, így a felhasználók jobban felismerhetik a biztonsági kockázatokat, és elsajátíthatják a helyes gyakorlatokat.

Hosszú távú cél, hogy a kutatás egy fenntartható és folyamatosan fejlődő biztonsági kultúra kialakításához járuljon hozzá. Ez a kultúra nemcsak az egyéni felhasználók mindennapi digitális biztonságát erősíti, hanem a vállalatok és intézmények működését is támogatja, elősegítve a tudatos, felelős és reziliens részvételt a digitális környezetben.

Összegzés

Napjainkban a humán tényező továbbra is meghatározó szerepet tölt be az információbiztonságban, és a felhasználók tudás-, attitűd- és viselkedésbeli sajátosságai alapvetően befolyásolják a szervezetek és egyének kiberrezilienciáját. A Security

Awareness Model empirikus vizsgálata igazolta, hogy a tudás–attitűd–viselkedés dimenziókra épülő, többdimenziós megközelítés alkalmas az információbiztonsági tudatosság komplex feltárására és mérésére. A modell erőssége, hogy nem csupán a technikai ismeretek meglétét értékeli, hanem képes feltárni a mögöttes kognitív és viselkedési mintázatokat is, ezáltal hozzájárulva a biztonságtudatosság mélyebb, strukturáltabb megértéséhez.

Az eredmények rámutattak arra, hogy a hallgatók megfelelően azonosítják a klasszikus kockázatokat és alapvető biztonsági elveket, azonban jelentős hiányosságok figyelhetők meg a szabályozási ismeretek, az új technológiákhoz való viszonyulás és a tudatos viselkedés dimenzióiban. E hiányosságok azt jelzik, hogy az információbiztonsági képzéseknek túl kell mutatniuk a puszta ismeretátadáson: szükség van az attitűdformálásra, a kritikus gondolkodás fejlesztésére és a biztonságtudatos döntéshozatal támogatására is. A modell validálása alátámasztotta annak mérési megbízhatóságát, ugyanakkor rávilágított a mérőtételek tartalmi pontosításának szükségességére, ami a jövőbeli kutatások egyik fő feladata lehet. A hosszú távú cél az adaptív, reziliens biztonsági kultúra kialakítása, amely képes alkalmazkodni a gyorsan változó technológiai és szabályozási környezethez, és hozzájárul a digitális ökoszisztéma fenntartható, biztonságos fejlődéséhez.

Felhasznált irodalom

Ahlan, Abdul Rahman – Lubis, Muharman – Lubis, Arif Ridho (2015): Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72, 361–373. Online: https://doi.org/10.1016/j.procs.2015.12.151

Alanazi, Marfua – Freeman, Mark – Tootell, Holly (2022): Exploring the Factors that Influence the Cybersecurity Behaviors of Young Adults. *Computers in Human Behavior,* 136, 107376. Online: https://doi.org/10.1016/j.chb.2022.107376

Alharbi, Talal – Tassaddiq, Asifa (2021): Assessment of Cybersecurity Awareness Among Students of Majmaah University. *Big Data and Cognitive Computing,* 5(2). Online: https://doi.org/10.3390/bdcc5020023

Aljohni, Wejdan et al. (2021): Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications,* 12(3), 276–281. Online: https://doi.org/10.14569/IJACSA.2021.0120334

Alqahtani, Mohammed A. (2022): Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences (Switzerland),* 12(5). Online: https://doi.org/10.3390/app12052589

Al-Janabi, Samaher – Al-Shourbaji, Ibrahim (2016): A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management,* 15(1). Online: https://doi.org/10.1142/S0219649216500076

Bak, Gerda et al. (2024): On the Way to Updating the Measurement of Information Security Awareness – A Literature Analysis. *Interdisciplinary Description of Complex Systems,* 22(3), 305–316. Online: https://doi.org/10.7906/indecs.22.3.6

Berek László et al. (2024): Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján. In Molnár György – Temesvári Zsolt – Wührl Tibor (szerk.): *XXXIX. Kandó Konferencia 2023*. Budapest: Óbudai Egyetem, 265–277. Online: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/25752/ksc_22.pdf?sequence=1&isAllowed=y

Blažič, Borka Jerman – Blažič, Andrej Jerman (2022): Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability (Switzerland),* 14(8). Online: https://doi.org/10.3390/su14084763

Hong, Yuxiang – Furnell, Steven (2021): Understanding Cybersecurity Behavioral Habits: Insights from Situational Support. *Journal of Information Security and Applications,* 57. Online: https://doi.org/10.1016/j.jisa.2020.102710

McCormac, Agata et al. (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior,* 69, 151–156. Online: https://doi.org/10.1016/j.chb.2016.11.065

Módné Takács, Judit – Pogátsnik, Monika (2024): The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z. *Acta Polytechnica Hungarica,* 21(6), 107–127. Online: https://doi.org/10.12700/APH.21.6.2024.6.6

Parsons, Kathryn et al. (2013): The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q). In Deng, Hepu – Standing, Craig (szerk.): *ACIS 2013: Information Systems: Transforming the Future: Proceedings of the 24th Australasian Conference on Information Systems.* RMIT University, 1–11. Online: https://bit.ly/4xeFK1v

Parsons, Kathryn et al. (2014): Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Parsons, Kathryn et al. (2017): The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers and Security*, 66, 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Répás József et al. (2024): HAIS-Q-tól a SAM-ig, a biztonságtudatosság mérésének modernizációja. *Hadmérnök,* 19(4), 183–198. Online: https://doi.org/10.32567/hm.2024.4.13

Répás József et al. (2025): Kisvállalkozások Nagy Kihívásai: Útmutató az Információbiztonsághoz. In Wührl Tibor (szerk.): *XL. Kandó Konferencia Kiadvány.* Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 179–186. Online: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/30380/Kiadv%C3%A1ny_Kando_XL_Konferencia.pdf

Shappie, Alexander T. – Dawson, Charlotte A. – Debb, Scott M. (2020): Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media,* 9(4), 475–480. Online: https://doi.org/10.1037/ppm0000247

Taha, Nashrawan – Dahabiyeh, Laila (2021): College Students Information Security Awareness: A Comparison Between Smartphones and Computers. *Education and Information Technologies,* 26(2), 1721–1736. Online: https://doi.org/10.1007/s10639-020-10330-0

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
21. évfolyam (2026) 1. szám 93–106.
DOI: 10.32567/hm.2026.1.6

Bodnár László,[1] Érczes Gergő,[2] Rácz Sándor[3]

A legjellemzőbb erdőtűzterjedési modellek áttekintő vizsgálata és elemzése

A Review and Analysis of the Most Characteristic Wildfire Spread Models

Absztrakt

Az erdőtűzterjedés az erdőtűzkockázat egyik központi eleme, hiszen meghatározza a tűz kiterjedését, a tűzveszélyt és a védekezési lehetőségeket is. A tűzterjedés alapját az elemi tűzformák adják, amelyek könnyen számíthatók. A tűzterjedés vizsgálata arra irányul, hogy a tűzfront milyen gyorsan halad az éghető anyag, az időjárási tényezők és a domborzat függvényében. A terjedési sebességgel szoros összefüggésben áll a tűzintenzitás, amely a tűzfront mentén felszabaduló energia mennyiségét fejezi ki, és gyakran a Byram-féle tűzfrontvonal-intenzitás segítségével számítják. A tűzintenzitás alapján következtetni lehet a lánghosszra, a hőterhelésre és a tűzoltási lehetőségekre. Az erdőtüzek hatásai azonban nem korlátozódnak csak és kizárólag a természetes környezetre, hanem gyakran érintik az épített környezetet is. Ennek értékelésére szolgál az épületkár-potenciál számításának vizsgálata, amely a tűzveszélyt az épületek kitettségével és sérülékenységével kapcsolja össze. Az épületkár-potenciál különösen az erdőhöz közeli lakott területek mentén jelentős. A cikk a fentiekben megfogalmazott, az erdőtűzterjedés szempontjából fontos tényezőket vizsgálja a releváns, nemzetközi szinten is elfogadott erdőtűzterjedési modellek segítségével. A cikk eredményeként nemcsak a modellek, hanem a tűzterjedésre vonatkozó számítási metódusok is megismerhetővé válnak.

Kulcsszavak: erdőtűz, tűzterjedés, elemi tűzforma, tűzintenzitás, épületkár-potenciál

[1] Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Mérnöki Tanszék, e-mail: bodnar.laszlo@uni-nke.hu
[2] Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Mérnöki Tanszék, e-mail: erces.gergo@uni-nke.hu
[3] Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi és Mentésirányítási Tanszék, e-mail: racz.sandor@uni-nke.hu

Abstract

Wildfire spread is one of the central issues in wildfire risk assessment, as it determines the spatial extent of the fire, the level of fire hazard, and the available options for suppression and mitigation. The basis of wildfire spread analysis lies in the elementary fire types, which can be described and quantified with relative simplicity. The study of fire spread focuses on the rate at which the fire front advances as a function of available fuels, meteorological conditions, and topography. Closely related to the rate of spread is fire intensity, which expresses the amount of energy released along the fire front and is commonly calculated using the Byram fire line intensity. Fire intensity provides a basis for estimating flame length, heat flux, and the feasibility of direct firefighting operations. However, the impacts of wildfires are not limited exclusively to the natural environment, as they frequently affect the built environment as well. The assessment of these impacts is addressed through the calculation of building loss potential, which integrates fire hazard with the exposure and vulnerability of structures. Building loss potential is of particular importance in residential areas located in close proximity to forested lands. This study systematically investigates the key factors identified as critically influencing wildfire spread by applying relevant and internationally established wildfire spread models. Beyond a comparative evaluation of these models, the paper also provides a detailed examination of the underlying computational approaches employed to quantify and predict fire propagation dynamics.

Keywords: wildfire, fire spread, elementary fire types, fire intensity, building loss potential

Bevezetés

Az erdőtüzek világszerte egyre komolyabb kihívást jelentenek, hiszen súlyos ökológiai, gazdasági és társadalmi következményekkel járhatnak.[4] Kialakulásuk és intenzitásuk a világ számos területén (így Magyarországon is) növekvő tendenciát mutat, amelyet az éghajlatváltozás, a szélsőséges időjárási események és a földhasználat változásai egyaránt erősítenek.[5] Az erdőtüzek nemcsak az erdei ökoszisztéma pusztulását idézhetik elő, hanem jelentős károkat okozhatnak az épített környezetben is, ezzel is veszélyeztetve az emberi életet és az anyagi javakat. A tűzterjedés mint folyamat kockázatos, a gyors tűzterjedés rövid idő alatt nagy területeket érinthet. A tűzterjedés sebessége és iránya gyakran nehezen számítható ki, hiszen azt az éghető anyag tulajdonságai,[6] az időjárási tényezők és a domborzat együttesen határozzák meg.[7] A gyors tűzterjedés növeli a tűzintenzitást és a hőterhelést, valamint csökkenti a hatékony beavatkozás lehetőségeit is.[8] A nem kontrollált erdőtűzterjedés különösen az erdőhöz közeli lakott területeken (*wildland-urban interface,* WUI) jelent veszélyt, ahol az épített környezet az erdőszegély mentén helyezkedik el. Az erdőtüzekhez kapcsolódó kockázatok kezelése

[4] Restás 2020; Debreceni 2023.
[5] Teknős–kórodi 2016.
[6] Xu et al. 2018.
[7] Nagy 2008.
[8] Sereg–Kerekes–Elek 2019.

ezért megbízható előrejelzési és értékelési módszereket igényel.[9] Az erdőtűzveszély és a tűzterjedés megértése alapvető feltétele a hatékony tűzmegelőzésnek és a sikeres oltásnak. Ennek hiányában az erdőtüzek hatásai súlyosabbak, illetve hosszú távon jelentős társadalmi és környezeti károkat is okozhatnak. Az erdőtűzterjedés témakörében jelen cikk célja bemutatni és matematikailag is igazolni az elemi tűzformákat, a tűzterjedés sebességét, a tűzintenzitást, illetve az épületkár-potenciál tűzvédelmi vonatkozásait. Ez a kutatás hazánkban eddig meglehetősen hiányos, holott a tűzkockázat értékelése erdészeti, tűzvédelmi és nemzetgazdasági szempontból is érdekes. A kutatási célok elérése érdekében összegyűjtöttük a téma releváns szakirodalmának hazai és nemzetközi tapasztalatait, valamint a kutatás során alkalmaztuk a mesterséges intelligencia adta lehetőségeket is. A GPT-5.1-es változatát használtuk a teljes szöveget érintően elsősorban táblázatok készítésére, írott szöveg pontosítására és szakirodalom keresésére. A vizsgált témát matematikai számításokkal is alátámasztottuk, emellett felhasználtuk saját eddigi tapasztalatainkat, amelyeket a témában hiteles szakértők[10] véleményeivel is kiegészítettünk.

Kutatásunkat az elemi tűzformák vizsgálatával kezdjük, amely megalapozza a tűzterjedés formáját. Ezt követően a kialakult tűzfront sebességét elemezzük, annak érdekében, hogy megállapítsuk, melyek a legfontosabb tényezői. A tűzintenzitás vizsgálata biztosítja a kutatásnak azt az égéselméleti hátterét, amelynek segítségével következtetéseket tudunk levonni a biomassza gyúlékonyságára és a tűzoltói taktikára. Végül elengedhetetlen az épített környezet tűzkockázatának is a vizsgálata, az emberi élet és az anyagi javak védelme érdekében.[11]

Elemi tűzformák vizsgálata

A tűzterjedés dinamikus folyamat, amelynek térbeli megjelenítésekor lényeges az, hogy a tűz a terjedése során milyen alakot (elemi tűzformát) vesz fel.

A szabadterületi tüzek általánosságban a következő tűzformákat vehetik fel:[12]

a) kör alak,
b) félkör alak,
c) egyszerű ellipszis,[13]
d) ellipszis pár,[14]
e) tojás forma,[15]
f) legyező forma.[16]

A *kör alakú* tűzforma szabadterületi tüzek esetén meglehetősen ritka. Ehhez minden esetben homogén biomassza, szélcsend, illetve sík terep szükséges. Bármely előbbi

[9] Debreceni 2019.
[10] Restás 2016; Sereg–Kerekes–Elek 2019.
[11] Vass et al 2024.
[12] Nagy 2008.
[13] Van Wagner 1969.
[14] Anderson 1983.
[15] Peet 1967.
[16] Byram 1959.

feltétel egy időben nem teljesül, a tűz már más alakot fog felvenni. Ez a tűzforma könnyen számítható, tűzterjedés esetén a kör kerületének képletét kell figyelembe venni, a leégett területek számításakor pedig a kör területét.

$$K = 2r\pi \quad (1)$$

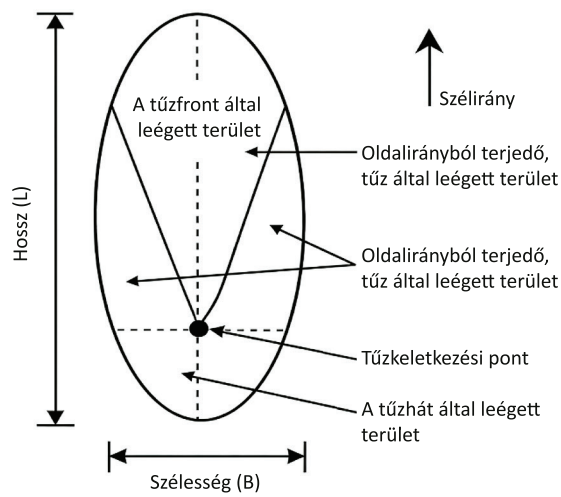
$$T = r^2\pi \quad (2)$$

A *félkör alakú* tűzforma szintén nagyon ritka. Ez a tűzforma a kör alakú tűzformán alapul, és kialakulásának feltételei is azonosak, azzal a különbséggel, hogy a tűz keletkezési helyén egy irányban nincs lehetőség tűzterjedésre. Ilyen lehet az, ha a tűz közvetlenül egy biomasszamentes terület mentén (például tűzpászta, földút) keletkezik. Ez a tűzforma is könnyen számítható, terjedés esetén a félkör kerületének képletét szükséges figyelembe venni, a leégett területek számításakor pedig a félkör területét.

$$K = r\ \pi{+}2\mathrm{r} \quad (3)$$

$$T = 0{,}5\ r^2\ \pi \quad (4)$$

Az *ellipszis alakú tűzforma* már eltér az előzőektől. Ebben az esetben jelentős befolyásoló tényező a szél iránya és sebessége, a domborzat, illetve a biomassza is. Elsősorban a szél adja a tűzforma „elnyújtott" alakját, ahogyan az 1. ábrán is látszik.



1. ábra: Ellipszis alakú tűzforma
Forrás: a szerzők szerkesztése VAN WAGNER *1969 alapján, Chat GPT 5.2 használatával*

Az összes tűzforma közül ez a legelfogadottabb, hiszen a szélirányban a tűz gyorsabban terjed, így az ellipszis hosszabb tengelye a széliránnyal párhuzamos. A rövidebb tengely viszont merőleges a szélirányra, hiszen a tűz lassabban terjed széllel szemben

vagy oldalszélben. Az ellipszis fókuszai a tűz keletkezési helye (tűzfészek) és az attól legmesszebbi elért pont. Ebben az esetben a tűz terjedési sebessége a széliránnyal megegyező irányban a leggyorsabb, illetve széllel szemben a leglassabb. A tűz alakja matematikailag könnyen leírható, jól mutatja azt, hogy változó környezeti feltételek esetén milyen a terjedő tűz alakja. Az ellipszis kerülete és területe a Ramanujan-féle megközelítés segítségével számolható, nem a legpontosabb eredményt adja, de megközelítő értékek megadására tökéletes.

$$K \approx \pi\left[3(a+b) - \sqrt{[(3a+b)(a+3b)]}\right] \tag{5}$$

Egyszerűbb megközelítés (kevésbé pontos, de gyorsabb):

$$K \approx \pi\left(\frac{3(a+b)}{2}\right) - \left(\frac{\sqrt{ab}}{2}\right) \tag{6}$$

Az ellipszis területe pontosan kiszámítható a következő képlettel:

$$T = \pi\frac{L}{2} * \frac{W}{2} \tag{7}$$

ahol:

- L = a tűz hosszú tengelyének hossza (szélirányban) (nagy tengely),
- W = a tűz rövid tengelyének hossza (széllel szemben) (kis tengely).

Az *ellipszis párok* mint tűzforma logikusan az egyszerű ellipszisen alapul. Ezek a tüzek azonban két vagy több ellipszis alakú tűzfrontot jelölnek, amelyek közös tűzfészekből vagy közel eső tűzfészkekből indulnak, de különböző irányokban, eltérő sebességgel terjednek. Az ellipszis párok nem feltétlenül szimmetrikusak, hiszen a terjedési sebesség és irány különböző környezeti paraméterektől (szél, terep, üzemanyag) is függ. Gyakori példa, hogy a szélirány hirtelen megváltozik, így a tűzfront kettéválhat, és két vagy több ellipszis alakú tűzfront keletkezik. Váltakozó irányú szél esetén kezdetben egy ellipszis alakú tűzfront terjed, például észak felé, majd 2 óra elteltével a szél délkeleti irányba fordul, és ekkor a tűzfront kettéválik: az eredeti tűzfront terjed tovább északi irányba, de lassabban, míg egy új tűzfront kelet felé veszi az irányt már gyorsabban. Ennek eredményeként két ellipszis pár alakul ki, amelyek különböző irányokban és sebességekkel terjednek. Domborzat szempontjából a következőképpen néz ki: egy tűz a völgyben terjed, ahol a szél felfelé gyorsítja a tűzterjedést, míg a völgy oldalain már lassabban terjed a tűz. Ennek eredményeként a tűzfront ismét kettéválik, és két ellipszis alakú tűzfront keletkezik.

Számítása nem egyszerű, hiszen több tényező is befolyásolja, például hogy minden ellipszis párt függetlenül karakterizálhatunk, illetve, hogy a tűzfrontok „összeérése" esetén a tűz területe és kerülete újraszámításra szorul.

$$A = \Sigma(\pi\frac{Li}{2} * \frac{Wi}{2}) \tag{8}$$

ahol:

- L1, L2: a hosszú tengelyek hossza (szélirányban),
- W1, W2: a rövid tengelyek hossza (széllel szemben).

Az ellipszis párok tehát a tűzterjedés komplex modelljei, amelyek változó környezeti feltételek mellett vagy több tűzfészek esetén alakulnak ki.

A *tojás alakú tűzforma* gyakori alak, amely nem szimmetrikus ellipszishez hasonlít, hanem inkább aszimmetrikus, egyoldalúan megnyúlt alakot ölt, akár egy tojás. Ez a forma általában akkor alakul ki, amikor a tűz terjedését egy irányban markáns tényezők (például erős szél, terep lejtése vagy egyoldalú üzemanyag-eltérés) befolyásolják, de a terjedés nem egyenletes minden irányban. A tojás alakú tűzforma fontos a tűz terjedésének megértésében, mert segít előre jelezni, hogy a tűz melyik irányba terjed a leggyorsabban, és hol alakíthatja ki a legnagyobb veszélyt. A tűz egy irányba megnyúlt, a másik irányba viszont rövidebb és szélesebb, mint egy szabályos ellipszis. A hosszabbik vége általában a széliránnyal vagy a lejtő irányával megegyezik ott, ahol a tűz gyorsabban terjed. A rövidebb vége a széllel szemben vagy a lejtővel szemben található, ahol a tűz terjedése logikusan lassabb. Az alak nem szimmetrikus, hiszen a tűz terjedési sebessége és irányai nem egyenlők. A tojás forma kialakulását okozhatja viharos szél, a domborzat lejtése, a heterogén biomassza (sűrűsége, eltérő szárazsága) jelenléte, illetve egyéb természeti akadályok is (például folyók, utak, sziklaszirtek). A tojás alakú tűzforma nem feleltethető meg pontosan egy matematikai ellipszisnek, de megközelíthető aszimmetrikus ellipszis modell segítségével. A tűz kerülete nem számítható ki egy egyszerű képlettel, mert a tűzalak nem szabályos. Területe esetén a tűz hosszabbik tengelye (L) a széliránnyal vagy lejtővel megegyező, a rövidebb tengelye (W) viszont ezekre merőleges (mint a szimmetrikus ellipszis).

$$T = \pi \frac{L}{2} * \frac{W}{2} \tag{9}$$

A *legyező alakú tűzforma* akkor alakul ki, amikor a tűz egy tűzfészekből vagy egy keskeny tűzfrontvonalból indulva terjed több irányba, és a terjedési sebesség a szélirányban vagy a terepviszonyok miatt szélesebb tűzfrontot hoz létre, mint egy szabályos ellipszis vagy tojás alak. Ez a forma jellemzően szélirányváltozás vagy terepakadályok esetén jelenik meg. A legyező alakú tűzfront széles, nyitott szögben terjed, és gyakran rövid idő alatt nagy területen pusztít, ami komoly kihívást jelenthet a tűzoltók számára. A tűz egy tűzkeletkezési helyről indul, majd széles, legyező alakban terjed tovább. A tűzfront nem záródik be, hanem nyitott, széles ívet alkot, akár egy legyező. A terjedés nem egyenletes: a szélirányban vagy a lejtő mentén a tűz gyorsabban, míg más irányokban lassabban halad. A tűzfront széleinek hossza és sebessége eltérő, mivel a környezeti feltételek (szél, terep, üzemanyag) változóak. Kialakulásának oka lehet a váltakozó szélirány vagy hirtelen szélcsend, a domborzat, vagy ha több kisebb kiterjedésű tűz összeérve markáns tűzfrontot eredményez. Váltakozó szél esetén egy tűz például északi irányba indul, de a szél keletre fordul, és a tűz keleti irányba már gyorsabban terjed, míg nyugat felé lassabban. Ennek eredményeként a tűzfront legyező alakot vesz fel, és széles területet érint. Ha a tűz sík területet érint, ahol nincs komolyabb szélsebesség, a tűz minden irányba egyenletesen terjed majd, és legyező alakú tűzfrontot hoz létre. A legyező formájú tűzfront nem feleltethető meg egyszerű geometriai alakzatoknak (például kör, ellipszis), mert a terjedés nem szimmetrikus. A tűz kerülete nem számítható egyszerű képlettel, mert a tűzfront nem szabályos.

A tűz megközelítő területét szektorterület-képlet alkalmazásával számíthatjuk ki (becsült összeg), ha feltételezzük, hogy a tűz egy szögben terjed.

$$A \approx \frac{\alpha}{360} \pi r^2 \tag{10}$$

ahol:

- α a legyező szöge (fokban),
- r a tűz átlagos terjedési távolsága a kiindulóponttól.

A legyező alakú tűz gyors terjedése miatt komoly kihívást jelent a tűzoltók számára.

Tűzterjedés sebességének vizsgálata

A felszíni tűzterjedés az erdőtüzek egyik alapvető folyamata, amely során a tűz a felszínen, az alsó biomasszaszinten (például avar, fű, bokrok, lehullott ágak) terjed. Ez a terjedési forma különösen fontos az erdőtüzek kezdeti szakaszában, valamint a tűz terjedésének megértésében, hiszen a felszíni tűz gyorsan növelheti a leégett területet, de átterjedhet a felső biomasszaszintre is (koronatűz). A felszíni tűzterjedés sebessége és intenzitása számos tényezőtől függ, például a biomassza jellegétől, a környezeti feltételektől (szélsebesség, hőmérséklet, páratartalom), valamint a terepviszonyoktól (lejtő, akadályok) is.

A felszíni tűzterjedés modellezése kulcsfontosságú a tűzveszély értékelése, a tűzoltási stratégiák kidolgozása és a tűzviselkedés előrejelzése szempontjából. Ebben a kontextusban Richard C. Rothermel 1972-ben kidolgozott egyenlete – a Rothermel-egyenlet – forradalmasította a felszíni tűzterjedés kvantitatív leírását. Ez az egyenlet matematikailag leírja, hogyan függ a tűzterjedési sebesség a biomasszától, a környezeti feltételektől és a domborzattól:

$$v_t = I_r \zeta \frac{1 + \Phi_w + \Phi_s}{\rho_b \varepsilon Q_{ig}} \tag{11}$$

- V_t = tűzterjedés sebessége,
- I_r = reakcióintenzitás,
- ξ = reakcióintenzitás aránya (szélcsend idején),
- Φ_w = légmozgási tényező,
- Φ_s = domborzati tényező,
- P_b = biomassza egységnyi térfogata,
- ε = effektív biomassza felhevülési aránya,
- Q_{ig} = biomassza gyulladáspontra hevítéséhez szükséges energia.[17]

A Rothermel-egyenlet lényege, hogy ha a tűzterjedés egyik tényezője kisebb, de egy másik tényezője nagyobb, akkor is kaphatunk hasonló tűzterjedési értéket, ezért vizsgálatunkban nem egy meghatározott gyúlékony biomasszatípust veszünk alapul,

[17] Rothermel 1972.

hanem a tűz fizikai megjelenésének paramétereire fókuszálunk. Az egyenlet alapján tehát a tűzterjedést befolyásolja a reakcióintenzitás, a reakcióintenzitás azon aránya, amely a szomszédos biomassza-részecskéket meggyújtja, a szél iránya és sebessége, a domborzat, a biomassza egységnyi térfogata, az effektív biomassza felhevülési aránya, illetve a biomassza gyulladáspontra hevítéséhez szükséges energia.[18]

A Rothermel-egyenlet elsőrendű a tűzökológia és a tűzvédelem területén, hiszen az egyenlet pontosan leírja a tűzterjedési sebességet a gyúlékony biomassza tulajdonságai (például méret, nedvesség, sűrűség), a környezeti paraméterek (például szélsebesség, lejtő) és a tűz intenzitása alapján. Az egyenlet alapja a tűzterjedési szimulációs rendszereknek is. A Rothermel-egyenlet építőeleme ezenfelül olyan széles körben használt tűzterjedési modelleknek, mint a BehavePlus vagy a FARSITE, amelyek segítik a tűzviselkedés előrejelzését és a tűzoltási döntésekhez szükséges információk nyújtását.[19] Az egyenlet segítségével tűzveszélytérképeket készítenek, amelyek segítik az erdőgazdálkodókat és tűzoltókat abban, hogy meghatározzák a legveszélyeztetettebb területeket és optimalizálják az erőforrások elosztását. Ezenkívül a Rothermel-egyenlet alapvető eszköz a tűzökológiai kutatásokban és az oktatásban, hiszen segít megérteni, hogyan befolyásolják a különböző tényezők a tűzterjedést.

A tűzintenzitás számításának lehetőségei

Tűzintenzitás alatt a tűzfrontvonal 1 m hosszán, 1 s alatt felszabaduló hőenergia mennyiségét értjük. Ez az érték kW/m-ben határozható meg. Erdőtüzek intenzitásának elemzésekor a Byram-féle tűzintenzitást *(Byram fireline intensity)* vehetjük alapul. A Byram-féle tűzintenzitás számítása az erdőtüzek vizsgálatának egyik alapeleme, amely azt fejezi ki, hogy mennyi hőenergia szabadul fel a tűzfront 1 m hosszán, 1 s alatt. Az eredeti meghatározást Byram adta meg.[20] Fontos, hogy jelen esetben a tűzintenzitás nem a teljes tűzre vonatkozik, hanem kifejezetten a tűzfrontvonal menti égés erejét mutatja meg. Számításakor olyan lényeges adatokat kapunk, amelyek felhasználhatók a helyes tűzoltási taktika kiválasztásakor[21] a tűz terjedésének előrejelzésekor, illetve az ökológiai hatások (például károsodott lombkorona) értékelésénél.[22] A tűzfront intenzitásának számítására a következő képlet áll rendelkezésre:[23]

$$I = H * w * R \tag{12}$$

- I = tűzintenzitás (kW/m) (helyenként FLI-nek jelölik),
- H = égéshő (kJ/kg),
- w = tűzfrontban elégett biomassza (kg/m^2),
- R = tűzterjedés sebessége (m/s).

[18] Bodnár 2021.
[19] Nagy 2008.
[20] Byram 1959.
[21] Tomka–Pántya 2022; Kanyó 2020.
[22] Nagy 2013.
[23] Byram 1959.

A fentiek szorzata adja meg tehát, hogy 1 m tűzfront mennyi hőt bocsát ki 1 s alatt. Ez a módszer közvetlenül még nem veszi figyelembe a lánghosszt. A tűzfrontban elégett biomassza kapcsán a következőket érdemes megjegyezni. Byram képletében a „*w*" a tűzfrontnál ténylegesen elégő biomassza tömegét jelöli: w [kg\cdotpm^{-2}].

Ez nem a teljes rendelkezésre álló biomassza mennyisége, hanem annak csak az a része, amely elégett a lángzónában a tűzterjedés ideje alatt. Ennek kiszámítása külön is lehetséges a következők szerint:

$$w = W * \eta \tag{13}$$

- „W" az éghető anyag tűzterhelése (kg*m^2),
- „η" az égés hatásfoka (0-1).

1. táblázat: A gyúlékony biomasszatípusok tűzterhelése

Gyúlékony biomassza típusa	**(W) [kg·m^{-2}]**
Fű (száraz)	0,3–0,8
Avartakaró (lombos erdő)	0,8–1,5
Tűlevelű avar	1,5–3,0
Cserjés	2–6

Forrás: a szerzők szerkesztése

Az égés hatásfoka függ a nedvességtartalomtól, a kiszáradási képességtől (1, 10 vagy 100 h-t követő kiszáradás), illetve az oxigénellátástól.

2. táblázat: Az égés hatásfoka egyes tűztípusoknál

Tűztípus	**(η)**
Gyors felszíni tűz	0,6–0,9
Nedves avar	0,3–0,5
Lassú, parázsló tűz	0,2–0,4

Forrás: a szerzők szerkesztése

Összességében tehát a tűzfrontvonal-intenzitás jelentősen függ a kialakult tűz típusától is, amit a 3. táblázat mutat be.

3. táblázat: Tűzfrontvonal-intenzitás egyes tűztípusok esetén

Tűz típusa	**Tűzfrontvonal intenzitása (kW/m)**
Alacsony intenzitású felszíni tűz	< 500
Közepes intenzitású felszíni tűz	500–2000
Nagy intenzitású felszíni tűz	2000–10 000
Lombkoronatűz	> 10 000

Forrás: a szerzők szerkesztése

A tűzintenzitás számításának másik lehetséges módja már a szabad területen kialakulni képes lánghosszt is figyelembe veszi (empirikus alapon). Számítási képlete a következő:

$$L = 0{,}0775 * I^{0{,}46} \tag{14}$$

- „L" a lánghossz,
- „I" a tűzintenzitás.

A képlet hatványfüggvényt tartalmaz, amelyben a 0,0775 érték egy illesztési konstans ($a = e^{\log a}$). Ez biztosítja, hogy az adott mértékegységek mellett a görbe átmenjen a mért adatok közepén. A 0,46 érték pedig az illesztett egyenes meredeksége, amely kifejezi, hogy a lánghossz nagyjából az intenzitás négyzetgyökénél kicsit gyengébben nő. Ez fizikailag azt jelenti, hogy a hő egy része radiációra, konvekcióra, illetve turbulens keveredésre megy el, és nem csupán „felfelé nyújtja" el a lángot. Az érték ezért nem 0,5 vagy 1, hanem 0,45–0,5 közé esik. A lánghossz a láng tengelye mentén mért hossza. A lánghossz mentő tűzvédelmi szempontból is mértékadó adat, hiszen meghatározható vele a helyes tűzoltási taktika. Ezt a 4. táblázat adatai mutatják meg.

4. táblázat: Helyes tűzoltási taktika az egyes lánghosszok esetén

Lánghossz (m)	**Alkalmazható tűzoltástaktika**
< 1,2	Kéziszerszámok segítségével
1,2–2,4	Hagyományos tűzoltás (gépjármű, szakfelszerelések)
2,4–3,5	Korlátozott beavatkozási képességek
> 3,5	Közvetlen oltás nem lehetséges (különleges gépjárművek, taktikai megoldások)

Forrás: a szerzők szerkesztése

Logikus tehát, hogy a tűzintenzitásból kiszámolható a láng becsült hossza. Példának okáért, ha:

I = 2000 kW/m, akkor a fenti (14)-es képlet alkalmazásával meghatározható, hogy a láng hossza megközelítőleg 2,6 m, ami kihívást jelentő, ám még kezelhető felszíni tűznek felel meg.

$$L = 0.0775 * 2000^{0{,}46} = 2{,}6\ \mathrm{m}$$

A tűzintenzitás tehát az erdőtüzek egyik legfontosabb tényezője, hiszen közvetlenül meghatározza a tűzfrontvonal mentén felszabaduló energia mennyiségét, ezzel meghatározva a tűzveszélyt is. A tűzintenzitás szoros kapcsolatban áll a lánghosszal, a hőterheléssel és azzal, hogy milyen beavatkozási, taktikai lehetőségek vannak egy adott vegetációtűznél. A tűzoltási taktikák megválasztása, az emberi élet és anyagi javak, valamint a védőzónák tervezése mind nagymértékben a tűzintenzitás becslésén alapul. Más szempontból a tűzintenzitás meghatározza a vegetáció vagy akár az épített környezet károsodásának mértékét. A következő fejezetben ezt vizsgáljuk meg részletesebben.

Az épületkár-potenciál számítása

Az épületkár-potenciál (*building loss potential,* BLP) egy kockázati mutató, amely azt fejezi ki, hogy egy adott erdőtűz – amely erdőhöz közeli lakott területek közelében terjed – mekkora valószínűséggel és milyen mértékben okozhat kárt az erdőszegély mentén található épületekben. Klasszikus értelemben nem fizikai képlet, mint a Byram-féle tűzintenzitás, hanem elsősorban integrált kockázati becslés, amely a tűz tulajdonságait és az épített környezet sérülékenységét kapcsolja össze. A BLP tehát megmutatja, hogy mekkora a valószínűsége annak, hogy az erdőszegély mentén található épületek a tűz által károsodnak vagy megsemmisülnek.

A BLP általában három fő komponens szorzataként vagy súlyozott összegként jelenik meg, úgymint tűzveszély, épületek kitettsége és épületek sérülékenysége. A *tűzveszély* mint kockázati komponens tartalmazza a tűzfrontvonal intenzitását,[24] az erdőterületen kialakulni képes láng hosszát, a tűz terjedési sebességét, illetve a tűz típusát (felszíni, korona). Az *épületek kitettsége* leírja, hogy hány épület érintett az erdőhöz közeli lakott területen (WUI), ezek milyen távolságra találhatók az éghető vegetációtól (erdőszegélytől), illetve, hogy milyen a lakott terület beépítettsége (például telepszerű, sűrű, ritka stb.). Az *épületek sérülékenysége* (WUI szempontból legfontosabb) komponenst befolyásolja többek között a tető fajtája (nem mindegy, hogy fa, zsindely vagy cserép), a falburkolat, a nyílászárók és a karbantartás is.

A BLP a következőképpen számolható:

$$BLP = I * E * V \tag{15}$$

- „I" – tűzintenzitás (például Byram),
- „E" – épületsűrűség / kitettség,
- „V" – épületsérülékenységi index.

A legtöbb alkalmazásban ezek normalizált (0–1) vagy kategóriás értékek.

A Byram-féle tűzfrontvonal-intenzitás a BLP egyik legfontosabb változója, hiszen meghatározza a lánghosszt, a sugárzó hőterhelés mértékét, az égő zsarátnokok (röptűz) keletkezését. Ezek pedig közvetlen hatással vannak a tetők meggyulladására, a nyílászárók károsodására, illetve a homlokzatok gyulladására. Az erdőtüzek kapcsán a BLP-t használják:

- evakuálás meghatározására,
- WUI-területek azonosításában és tűzvédelmi tervezésben,
- biztosítási és kárbecslési modellekben,
- tűzmegelőzési programok értékelésére.

A BLP tehát azt mutatja meg, hogy egy erdőtűz mekkora veszélyt jelent az épített környezetre. Számítása a tűzveszélyt (például Byram-féle tűzintenzitás), az épületek kitettségét és azok sérülékenységét egyesíti. Erdőtüzeknél különösen a WUI-területeken kulcsfontosságú ez a mutató. Tulajdonképpen nem egyetlen képlet, hanem

[24] Byram 1959.

egy döntéstámogató keretrendszer, amelynek nem a pontosság az elsődleges célja, hanem a kockázatok helyes felismerése. Tűzkockázatát természetesen befolyásolja az épület típusa,[25] a választott építőanyag[26] és a tűzvédelmi követelmények is.[27]

Bár a kutatás ezen fejezetében elsősorban az épített környezet sebezhetőségére koncentráltunk, fontos még megemlíteni az erdőtűz káros ökológiai hatásait is. Ide tartozhatnak többek között az erdei talaj károsító hatásai,[28] a vízminőség romlása,[29] a káros vagy üvegházhatású gázok kibocsátása.[30]

Következtetések

Az erdőtűzterjedés vizsgálatának eredményeként megállapítottuk, hogy a tűzterjedés alapját az elemi tűzformák adják, hiszen ezek határozzák meg a tűzterjedés fontos tényezőit. A tűzterjedés sebességének vizsgálata kulcsfontosságú a tűz időbeli lefolyásának és a veszélyeztetett területek előrejelzéséhez, mivel szorosan függ az éghető anyag tulajdonságaitól, az időjárástól és a domborzattól. A terjedési sebességgel szoros kapcsolatban áll a tűzfront mentén felszabaduló energia mennyiségét kifejező tűzintenzitás. A tűzintenzitás segítségével következtetni lehet a lánghosszra, a hőterhelésre és a közvetlen tűzoltási taktikai lehetőségekre is. Az erdőtüzek nemcsak a természetes környezetet érintik, hanem az épített környezetet is veszélyeztethetik. Ennek értékelésére szolgál az épületkár-potenciál számítása, amely a tűzveszélyt az épületek kitettségével és sérülékenységével is összekapcsolja. Az erdőtűzterjedés komplex értelmezése így egyszerre támogatja a hatékony mentő tűzvédelmi döntéseket és a kockázatalapú tervezést is.

Felhasznált irodalom

Anderson, Hal (1983): *Predicting Wind-Driven Wildland Fire Size and Shape.* Ogden, UT: US Department of Agriculture, Forest Service, Intermountain Forest and Range Experiment Station. Online: https://doi.org/10.5962/bhl.title.69035

Bodnár László (2021): *Az erdőtüzek oltásának hatékonyságát növelő módszerek kutatása és fejlesztése*. PhD-disszertáció. Budapest: Nemzeti Közszolgálti Egyetem. Online: https://doi.org/10.17625/NKE.2021.020

Byram, George (1959): ***Combustion of Forest Fuels.*** In Davis, Kenneth P. (szerk.): *Forest Fire: Control and Use*. New York: McGraw-Hill, 61–89. Online: www.frames.gov/documents/behaveplus/publications/Byram_1959_CombustionOfForestFuels.pdf

[25] Komlai–Restás–Kerekes 2021.
[26] Csorba et al. 2025.
[27] Kerekes–Gyöngyössy–Elek 2017.
[28] Hajdu et al. 2024.
[29] Liptai–Engloner 2024.
[30] Teknős–Debreceni 2022.

Csorba, Kristóf et al. (2025): Monitoring of Historical Structural Materials with Computed Tomography. *Structural Concrete,* 1–13. Online: https://doi.org/10.1002/suco.202400149

Debreceni Péter (2019): Erdőtűz időjárási index használata az erdőtűz megelőzésben. In Facskó Ferenc – Király Gergely (szerk.): *VII. Kari Tudományos Konferencia a konferencia előadásainak és posztereinek kivonatai*. Sopron: Soproni Egyetem Kiadó, 16.

Debreceni Péter (2023): Kihívások és lehetőségek a hazai erdőtűz megelőzésben egy új európai megközelítés tükrében. *Védelem Tudomány,* 8(Ksz.), 119–127. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13887/11323

Hajdu Flóra et al. (2024): Az erdőtűz talajra gyakorolt hatásainak vizsgálata számítógépes szimulációval I. Modellek vizsgálata. *Tűzvédelem,* 31(1), 5–8.

Kanyó Ferenc (2020): Középmagas társasházi tetőtűz tűzoltási taktikája. *Védelem Katasztrófavédelmi Szemle,* 27(4), 49–53. Online: www.vedelem.hu/letoltes/ujsag/v202008.pdf?5

Kerekes Zsuzsa – Gyöngyössy Éva – Elek Barbara (2017): Tűzoltó kábelek műanyag burkolatának új és hagyományos vizsgálati módszereinek összehasonlító elemzése. *Védelem Tudomány,* 2(3), 24–36. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13129/10598

Komlai, Krisztina – Restás, Ágoston – Kerekes, Zsuzsanna (2021): Fire Resistance Thermodynamic Test of Self-supporting Double Skin Metal Faced Sandwich Panels. In Bodnár, László – Heizler, György (szerk.): *Proceedings of the Fire Engineering & Disaster Management Prerecorded International Scientific Conference.* Budapest: Nemzeti Közszolgálati Egyetem, 179–184. Online: https://kvi.uni-nke.hu/document/kvi-uni-nke-hu/440-konferencia.pdf#page=181

Liptay Zoltán – Engloner Attila (2024): A klímaváltozás lehetséges hatásai a nagy folyóink vízminőségére: a vízminőségi modellezés peremfeltételeinek klímaparaméterezése. *Légkör,* 69(Ksz.), 30–36. Online: https://doi.org/10.56474/legkor.2024.K.5

Nagy Dániel (2008): *Erdőtüzek megelőzési és oltástechnológiai lehetőségeinek vizsgálata*. PhD-disszertáció. Sopron: Nyugat-magyarországi Egyetem. Online: http://doktori.uni-sopron.hu/id/eprint/30/1/disszertacio.pdf

Nagy Dániel (2013): *Erdőtűz megelőzési intézkedések erdővédelmi, tűzterjedési és ökonómiai paramétereinek kidolgozása*. Sopron: Nyugat-Magyarországi Egyetem.

Peet, Geoffrey Brian (1967): The Shape of Mild Fires in Jarrah Forest. *Australian Forestry,* 31(2), 121–127. Online: https://doi.org/10.1080/00049158.1967.10675433

Restás, Ágoston (2016): The Examination of the Economical Effectiveness of Forest Fire Suppression by Using Theoretical Fire Spread Models. *Academic and Applied Research in Military and Public Management Science,* 15(1), 85–92. Online: https://doi.org/10.32565/aarms.2016.1.8

Restás Ágoston (2020): Az erdőtüzek intenzitásának változása a globális klímaváltozás hatására. In Földi László – Hegedűs Hajnalka (szerk.): *Éghajlatváltozás okozta kihívások és lehetséges válaszok*. Budapest: Ludovika, 91–106. Online: https://doi.org/10.36250/00833_05

Rothermel, Richard (1972): *A Mathematical Model for Predicting Fire Spread in Wildland Fuels.* Ogden: U.S. Department of Agriculture, Intermountain Forest and Range Experiment Station. Online: https://research.fs.usda.gov/download/treesearch/32533.pdf

Sereg Adrienn – Kerekes Zsuzsanna – Elek Barbara (2019): Az erdők környezeti vegetációjának hatása a tűzesetekre, a megelőzés egyes lehetőségei. *Védelem Tudomány,* 4(4), 74–90. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13362/10788

Teknős, László – Debreceni, Krisztina, A (2022): Disaster Management Aspects of Global Climate Change. In Molnár, András – Wenczel, Dóra (szerk.): *Third International Conference on Effective Response: Conference Proceedings.* Budapest: Magyar Vöröskereszt, 45–55.

Teknős László – Kóródi Gyula (2016): A globális éghajlatváltozás biológiai kockázatainak elemzése, hatásainak vizsgálata a katasztrófavédelemre I. *Bolyai Szemle,* 1(1), 115–130. Online: www.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-216-1.original.pdf

Tomka Péter – Pántya Péter (2022): Elsődleges katasztrófavédelmi, tűzoltósági beavatkozások épített környezetben. *Polgári Védelmi Szemle,* 14(Ksz.), 143–152. Online: https://mpvsz.hu/pv_szemlek/pvszemle2022/index.html

Van Wagner, C. E. (1969): A Simple Fire-Growth Model. *The Forestry Chronicle,* 45(2), 81–142. Online: https://pubs.cif-ifc.org/doi/epdf/10.5558/tfc45103-2

Vass, Gyula et al. (2024): Results and Future of Disaster Management Research in the System of Law Enforcement Sciences. *Belügyi Szemle,* 72(5), 909–927. Online: https://doi.org/10.38146/bsz-ajia.2024.v72.i5.pp909-927

Xu, Qiang et al. (2018): Evaluate the Flammability of a Pu Foam with Double-Scale Analysis. *Journal of Thermal Analysis and Calorimetry,* 133, 3329–3337. Online: https://doi.org/10.1007/s10973-018-7494-2

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 1. szám 107–124.
DOI: 10.32567/hm.2026.1.7

Csóka Attila,[1] Kantár György[2]

ABV-megfigyelés mint szolgáltatás az állandó strukturált együttműködés rendszerében

Hazai érdekek és perspektívák

CBRN Surveillance as a Service within the Framework of Permanent Structured Cooperation

Domestic Interests and Perspectives

Absztrakt

Az Európai Unió tagországainak védelmi célú együttműködése számos területet lefed, amelynek részeként az atom, biológiai, vegyi felderítés fejlesztése és a vonatkozó helyzetkép kialakítása érdekében több közép-európai nemzet közös erőfeszítést fejt ki az ABV-megfigyelés mint szolgáltatás projekt keretében. A szerzők összefoglalják a projekt célkitűzéseit, eredményeit, problémákat azonosítanak, valamint elemzik a kifejlesztendő rendszer, illetve annak elemei hazai hasznosíthatóságának lehetőségeit.

Kulcsszavak: PESCO, ABV, EDA

[1] Ezredparancsnok-helyettes, MH Sodró László 102. Vegyiharc Ezred.
[2] Kiemelt referens főtiszt, Honvéd Vezérkar Haderőtervezési Csoportfőnökség Fegyvernemi Képességtervező Főnökség.

Abstract

The defence cooperation between European Union member states covers a number of areas, including the development of chemical, biological, radiological and nuclear detection capabilities and the development of the CBRN Operational Picture. Several Central European nations are working together on this as part of the CBRN Surveillance as a Service project. The authors summarise the objectives and results of the project, identify problems, and analyze the potential for national-level application of the system and its components.

Keywords: PESCO, CBRN, EDA

Bevezetés

A Krím 2014-es orosz megszállásától kezdve tapasztalhatjuk az európai államok biztonságpercepciójának változását, beleértve a hagyományos összhaderőnemi hadviselés jelentőségének újra felértékelődését, illetve a hibrid hadviselésben rejlő lehetőségek megértését. A bevezető gondolatot alátámasztja az állandó strukturált együttműködés (Permament Structured Cooperation, PESCO) lehetőségének kiaknázása. A Lisszaboni Szerződés[3] 42(6) bekezdése és annak 10. számú protokollja[4] már korábban is lehetővé tette a tagállamok védelmi célú együttműködését a PESCO keretében, azonban ezt a lehetőséget évekig nem aktiválták.

A tagállamok védelmi célú együttműködését – a Krím megszállását követően – az EU 2016-os globális stratégiája[5] már hangsúlyozza, ennek megfelelően a PESCO aktiválására 2017-ben sor került. 2017. december 11-én az Európai Unió Tanácsa meghozta a CFSP 2017/2315 számú döntését,[6] amellyel a tagállamok megalapítják a PESCO-t, rögzítve benne az önkéntes 25 induló tagállamot, közöttük Magyarországot is. A döntés elfogadja a 10. számú protokollban rögzítettnek megfelelően a főbb területeket, amelynek 2. cikkelye alapján a részt vevő államok kötelezettséget vállalnak, hogy

„védelmi berendezéseiket a lehető legnagyobb mértékben közelítik egymáshoz, különösen katonai szükségleteik meghatározásának összehangolásával, védelmi eszközeik és képességeik összevonásával […], konkrét intézkedéseket hoznak katonai erejük rendelkezésre állásának, interoperabilitásának, rugalmasságának és bevethetőségének fokozása érdekében […], részt vesznek az Európai Védelmi Ügynökség keretében nagyszabású közös vagy európai felszerelési programok kidolgozásában".[7]

[3] Consolidated Version of The Treaty on European Union 2012.
[4] Európai Unió 2008.
[5] European Commission 2016.
[6] Council Decision (CFSP) 2017/2315.
[7] Európai Unió 2008: 2 cikk *b)–e).*

A területek céljainak elérése érdekében az aláíró államok összesen húsz további ambiciózus és rögzített kötelezettségvállalást tettek.[8] Az első PESCO-ülés 2018. március 3-án volt, a tagállamok formálisan elfogadták a kezdeti 17 projektet. Napjainkban a tagállamok hét területen működnek együtt, beleértve az öt műveleti teret (szárazföld, levegő, tenger, kiber, űr), valamint a kiképzési létesítményeket, továbbá a stratégiai támogató tényezőket/erősokszorosítókat, a területeken összesen 75 projektet folytatva.

Az ABV (atom, biológiai, vegyi) figyelés mint szolgáltatás (Chemical, Biological, Radiological and Nuclear Surveillance as a Service, CBRN SaaS) kezdeményezést a PESCO-projektek második hullámában, 2018. november 19-én fogadták el abból a célból, hogy a részt vevő országok kifejlesszenek olyan ember által irányított, de pilóta nélküli földi és légi érzékelő hálózatot, amely kompatibilis a tagállamok korábbi, idősebb rendszereivel, ezáltal lehetővé téve az ABV-helyzetkép kialakítását, pontosítását az EU-missziók és -műveletek támogatása érdekében.

A tanulmány bemutatja a PESCO CBRN SaaS projekt fejlődését, a kezdeményezést támogató további programokat, az ABV-helyzetkép kialakítására vonatkozó koncepciót, esettanulmány-alapú módszertannal elemzi az adatok továbbításának megvalósulását, az ABV-helyzetkép kialakításához kulcsfontosságú adatátviteli kapacitás korlátait a valós idejű ABV-megfigyelésben, továbbá javaslatot tesz a Magyar Honvédség általi felhasználhatóságra, különös tekintettel a rendszeresített és használatban levő drónok túldiverzifikáltságának elkerülésére.

A PESCO CBRN SaaS projekt megvalósulása

Az ABV védelmi terület növekvő fontosságát jelzi, hogy az Európai Unió 2023-ban kiadott képességfejlesztési prioritásai *(The 2023 EU Capability Development Priorities)* tárgyú dokumentum hat fő területen (az öt műveleti tér és a támogató tényezők) 22 fejlesztési irányt határoz meg, amelyek között, a korábbi kiadással ellentétben, megtalálható az ABV-védelem *(CBRN defence)*.[9] A légi sugárfelderítés önmagában, helikopterek igénybevételével a 80-as évektől már elfogadott eljárás volt, azonban a mérés pontossága nem volt meggyőző, azt meg kellett erősíteni helyszíni mérésekkel. A technológia fejlődésével Zelenák és társai 2009-ben publikálták a légi sugárfelderítés alkalmazhatóságának vizsgálatát sugárforrások felkutatása, valamint szennyezett terepszakaszok határainak felmérése esetén, amelynek alapja egy fejlesztés alatt lévő, helikopterre integrálható légi sugárfelderítő konténer volt. Ekkor még a hordozó eszközök képességei, valamint a detektorok mérete, súlya miatt nem vehették figyelembe a drónok nyújtotta lehetőségeket.[10]

A különböző repülő és földi drónok elterjedésével a megfelelő detektorok integrálása, valamint az adatok továbbításának megoldása vált kulcskérdéssé. Pavlovsky és társai 2018-ban kutatták, hogyan lehet pilóta nélküli légi járműre (*unmanned aerial vehicle,* UAV) szerelt gamma-spektrométerekkel mérve, helyszíni adatösszesítéssel

[8] *Binding Commitments* [é. n.].
[9] European Defence Agency 2023.
[10] Zelenák et al. 2009.

háromdimenziós sugárzástérképet létrehozni.[11] Keith David McManus, aki részt vett Pavlovsky kutatásában is, 2019-ben publikált értekezésében igazolja az UAV-alapú sugárfelderítés végrehajthatóságát különösen röntgen- és gamma-sugárforrások esetén, részletezi a kis méretű detektorok integrálhatóságának körülményeit/feltételeit.[12]

A fenti kutatások eredményeikkel bizonyították az UAV-platformra integrált sugárfelderítés végrehajthatóságát, azonban tudományos értékük és a felhasználhatóságuk ellenére nem hasonlíthatók össze a PESCO-projekttel, mivel a kutatások elsősorban *platformcentrikus* megközelítést alkalmaztak, míg a CBRN SaaS rendszerszintű, szolgáltatásalapú megközelítést képvisel.

A PESCO CBRN SaaS projekt koordinátora Ausztria, a részt vevő tagok Ausztria mellett Horvátország, Franciaország, Magyarország és Szlovénia, továbbá megfigyelőként vesz részt Csehország és Olaszország. Molnár Anna és Szabolcs Laura változó geometriaként jellemzi azt a differenciált integrációt, amelynek megnyilvánulásaként azok az országok kapcsolódnak be adott projektekbe, amelyek között a bizalom, de különösen az érdekek már korábban összhangban voltak.[13] A CBRN SaaS esetében szembetűnő a hasonlóság a Közép-Európai Védelmi Együttműködéssel (Central European Defence Cooperation, CEDC), amelynek tagjai Ausztria, Csehország, Horvátország, Magyarország, Szlovákia és Szlovénia, ami már korábban azonosított közös érdekeket feltételez.

A tagországoknak lehetőségük van csak azokban a PESCO-projektekben részt venni, amelyek a nemzeti érdekeket tekintve megfelelők, s azokat támogatva valós hozzáadott értékük van, ezzel minimalizálva a költségeket, azaz a projektek a kisebb államok szinergiakeresését egészíti ki az uniós források elérhetőségének biztosításával. A PESCO-projekt politikai szintű elköteleződést biztosít, azonban az ambíciók teljesítése érdekében szakmai, műszaki, pénzügyi hátteret, valamint a szabványosítás és az interoperabilitás jelentette kihívásokat is meg szükséges oldani.

Az Európai Védelmi Ügynökség (European Defence Agency, EDA) kétféle, úgynevezett A kategóriás és B kategóriás programot működtet. Az A kategóriás, közös beruházási programok több tagállam részvételével, befektetési alapként működnek, amelyből az egyes projekteket finanszírozzák. Az alapba befizető összes tagállam dönt arról, hogy a pénzt mely projektekre fordítják, és mindannyian döntenek a szerződések odaítéléséről. Az A kategóriás projekt biztosítja, hogy egy adott programhoz minden EDA-tagország hozzájáruljon, központi forrásból, egységes elvekkel és szigorúbb jóváhagyási mechanizmussal menedzselve. A B kategóriás projektek nagyobb rugalmasságot adnak, legalább két ország részvételével már indíthatók, a tagok maguk szervezik a finanszírozást és a menedzsmentet, nem építenek központi költségvetésre.[14]

A PESCO CBRN SaaS projekt támogatása érdekében az EDA egy B kategóriás tükörprojektet indított 2019-ben, szintén CBRN SaaS elnevezéssel, amelyhez az Ügynökség biztosítja a projektmenedzsert, aki szakmai tapasztalatát tekintve ABV-védelmi szakember. Az EDA-projektben Ausztria mellett Horvátország, Magyarország és Szlovénia vesz részt. Habár a PESCO-projektben Franciaország is tag, az EDA-projektben

[11] Pavlovsky et al. 2018.
[12] McManus 2019.
[13] Molnár–Szabolcs 2020: 100.
[14] European Defence Agency 2010.

nem vesz részt, mindemellett a csatlakozási lehetőség más EDA-tagállamok számára is nyitott. Az EDA és a négy részt vevő állam közötti projektmegállapodás 2019. december 12-én lépett hatályba. A szakmai vonalat egy ipari konzorcium képviseli, amelyhez szintén szabadon csatlakozhatnak a részt vevő államok ipari szereplői, és amely konzorciumot az Osztrák Technológiai Intézet (Austrian Institute of Technology, AIT) vezeti. Magyarország részéről a konzorciumban a BHE Bonn Hungary Elektronikai Kft., valamint a Gamma Műszaki Zrt. vesz részt. A projekt szerződését a hozzájáruló tagállamok nevében az EDA, a konzorcium nevében az AIT írta alá 2020. november 19-én.[15]

A B kategóriás projekt természetét tekintve az EDA nem biztosít hozzáadott forrást a tagok 3,7 millió eurós befizetésén túl, így az ipari konzorcium fejlesztési költségeinek támogatása érdekében egy újabb, harmadik projekt indítására volt szükség. Az Európai Védelmi Ipari Fejlesztési Program (*European Defence Industrial Development Programme*, EDIDP) 2019–2020 között 500 millió eurót biztosított a nevében is meghatározott célra, így ez gyakorlatilag a későbbi Európai Védelmi Alap (European Defence Fund, EDF) előszobájának tekinthető.[16] A további források elérése érdekében, az EDA-projekt támogatásának céljából az EDIDP 2020-tól 30 hónapos időtartamban ABV-felderítési és -megfigyelési rendszer (*CBRN reconnaissance and survaillance system,* CBRN RSS) néven projektet indított az AIT által vezetett ipari konzorcium részére. A projekt teljes költségvetése 8 273 521,27 euró, amelyből a maximális EU-hozzájárulás 6 739 999,50 euró volt.[17]

Az ipari konzorcium tagjai a már meglévő termékeik, fejlesztéseik további fejlesztésével, specializálásával és összehangolásával kívántak a kihívásnak eleget tenni. Példaként hozható a BHE, amely a piacon levő TCP/IP-alapú MIMO adatátviteli rádióit (decentralizált hálózatok kiépítésére alkalmas modulokat) finomította és szabványosította úgy, hogy a drónok érzékelői által gyűjtött ABV-adatokat biztonságosan továbbítsa.[18]

A CBRN SaaS-rendszer alapelve, hogy ABV-fenyegetéssel érintett műveleti területeken, valamint egy esetleges ipari katasztrófa során radiológiai vagy vegyi kibocsátás esetén, az incidens helyszínén tevékenykedő parancsnokokat olyan eszközökkel lássa el, amelyek gyors és megbízható információt szolgáltatnak, ezáltal segítve a műveleti tervezést és reagálást, valamint katasztrófákat követően a következmények felszámolását.

A projekt keretében a CBRN SaaS-rendszer a kereskedelmi és katonai forgalomban elérhető (*commercial off-the-shelf, military off-the shelf,* COTS, MOTS) megoldásokat integrálja és fejleszti tovább egy új, magasabb szintű ABV-felderítési képességgé. Az operátorok egyszerűen használható, távolról működtethető megoldást kapnak az ABV-fenyegetések észlelésére és monitorozására az ABV-fegyverek bevetését követően.

[15] Pusch 2021.
[16] European Commission [é. n.].
[17] European Commission 2021.
[18] BHE 2024.

A CBRN SaaS-koncepció

Az ambíció szerint hogyan is épül fel a CBRN SaaS? A rendszer négy szintből áll. Az első szintet képviselik maguk az ABV-érzékelőkkel ellátott, adatok mérésére, továbbítására, eseteként ABV-mintavételre alkalmas drónok. Az eszközök irányítása a vezérlő elem (*control element,* CE) által történik, a CE-k adatait a közös vezérlő elem (*common control element,* CCE) összesíti, és a teljes elemzést, az interoperabilitás megvalósítását az adatösszesítő elem (*data fusion cell,* DFC) végzi.

A drónok feladata, hogy a speciálisan erre a célra fejlesztett szenzorokkal a potenciális szennyezett területen méréseket végezzenek, és detektálják a különböző ipari toxikus anyagok, mérgező harcanyagok jelenlétét, valamint információt nyújtsanak a radioaktív izotópok által okozott sugárszintről/szennyezettségről. A mért adatokon felül nagy felbontású élőkép továbbítására is képesek a vizuális elemzés és helyzetfelmérés érdekében.

Az AIT három különálló, pilóta nélküli egységet fejleszt annak érdekében, hogy azokkal a szennyezett terepszakaszra belépve méréseket hajtsanak végre detektálás, azonosítás és monitorozás céljából. Mindegyik pilóta nélküli egység vegyi és radiológiai szenzorokkal, detektorokkal felszerelt, amelyeket modulárisan integráltak, így cserélhetők az adott helyzet vagy fenyegetés követelményeinek megfelelően.

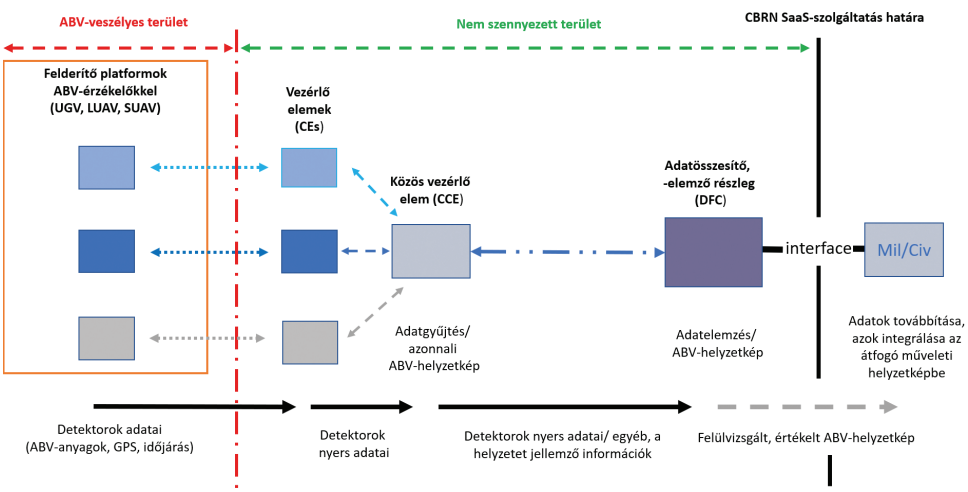
Az eszközök fejlesztésének kiindulási platformjai az osztrák Schiebel cég nagy méretű forgószárnyú eszköze (*large unmanned aerial system,* LUAS), a szlovén OneDrone kis méretű merev szárnyú drónja (*small unmanned aerial system,* SUAS), továbbá a horvát DOK-ING cég földi eszköze (*unmanned ground system,* UGS). Az eszközök közös előnye, hogy azok európai, sőt kifejezetten közép-európai fejlesztésűek és gyártásúak. Korunk biztonságpolitikai és gazdasági környezetében különösen fontosak a teljesen európai fejlesztésű, gyártású és fenntartású eszközrendszerek mind beszerzésbiztonsági, mind logisztikai, de interoperabilitási megközelítésből is, ezeken felül a fejlesztés során összegyűlt gyakorlati tapasztalat előnyt jelent a jövőbeli rendszerek kialakítása és fejlesztése szempontjából.

A CE-k fő célja a drónok irányításán túl azok feladatainak megtervezése (repülési útvonal a kijelölt szektorban az ABV-felderítés leghatékonyabb kivitelezése érdekében), a forrásszintű mérési adatok gyűjtése. A CE-k és a drónok közötti hatótávolság alapvetően két fő tényezőtől függ: a drónok maximum hatótávolságától, valamint a detektor által mért adatok interfészen keresztüli adattovábbítási képességétől. Az adattovábbítás hatótávolságának növelése egy másik, átjátszó szerepkörben alkalmazott drón bevonásával növelhető. A CE-k személyzete magában foglalja a drónpilótát, valamint az ABV-felderítésben jártas kiképzett szakállományt egyaránt.

A CCE összesíti a vezérlő elemek által küldött adatokat, azokat megjeleníti és egyben azonnali értékelést végez, valamint továbbítja az adatokat. A rendszer egyik fő követelménye, hogy legyen képes akár 50 km távolságból eljuttatni a mérési adatokat adatredukálással. A CCE által nyomon követhetők a drónok által megtett mérési útvonalak, valamint a mérési pontok. A szennyezettség mértékét a rendszer vizuálisan is képes megjeleníteni színek alkalmazásával (zöld–sárga–piros színkódok rendre: nincs szennyezés – mérsékelt szennyezés – nagy mértékű szennyezés). Az 1. ábra bemutatja a CCE által készített helyzetképet.

1. ábra: A közös vezérlőelem (CCE) helyzetképe
Forrás: a szerzők felvétele

A CCE az adatokat az adatösszesítő és -elemző részleg számára továbbítja. A hasznos mérési információ megérkezik a DFC-be, ahol azokat az EU- és NATO-tagállamok által is alkalmazott szoftverekkel vizsgálják, elemzik és értékelik.



2. ábra: PESCO CBRN SaaS koncepció
Forrás: a szerzők szerkesztése

Az elemzést követően a DFC létrehozza a felülvizsgált, értékelt ABV-helyzetképet, amelyet továbbít a támogatott, akár civil, akár katonai szervezetnek. A PESCO CBRN SaaS műveleti koncepciója a 2. ábrán látható.

Katonai felhasználás esetén az automatizált harcvezető rendszerben *(battlefield management system)* vizuális és mérési adat szintjén is megjelenik az aktuális ABV-helyzetkép, amelynek elemzésével a szaktisztek olyan információkkal láthatják el a művelet vezetéséért felelős parancsnokot, amely elősegíti a döntéshozatalt a művelet hatékony folytatása és az erők megóvása érdekében.

Az ABV-helyzetkép megjelenítése azonban nem csupán a parancsnok döntéshozatalát segíti elő, hanem ezzel egy időben a szennyezett terepszakaszon vagy azok közelében tartózkodó alegységek részére is azonnali riasztást és helyzetképet ad, ezáltal késlekedés nélkül bevezethetők azok a rendszabályok (ABV-védelmi szintek növelése, egyéni ABV-védelmi felszerelések, illetve kollektív ABV-védelmi eszközök alkalmazása), amelyekkel tovább folytatható a harc ABV-környezetben, valamint elkerülhető a további ABV-szennyezés vagy élőerő-veszteség.

ABV-felderítő platformok

Schiebel S100 LUAS

Az S100 Camcopter önállóan irányítható, többcélú eszköz vertikálisan fel- és leszálló (*vertical take-off and landing,* VTOL) rotoros drón, amelyet különböző katonai, valamint ipari feladatok végrehajtására terveztek. A jármű kialakításakor elektromos és üzemanyagcellás hibrid meghajtást is alkalmaztak. A maximális hatótávolság adatkapcsolat alapján 200 km.[19] Az eszköz a 3. ábrán látható.

A Camcopter S100 különböző célokra használható, különböző függesztmények alkalmazásával. A drón optikai és infravörös kameráival nappal és éjszaka is képes felderítést és megfigyelést végrehajtani, nagy felbontású fényképeket készíteni és lézeres távolságméréssel (*light detection and ranging,* LiDAR) pontfelhőt generálni, amely segítségével pontos 3D-s modelleket hozhatunk létre, ami hasznos lehet katasztrófa sújtotta helyszínek feltérképezésénél. Katasztrófaelhárítás és mentési műveletek során az eszköz gyorsan és hatékonyan juttathat el felszereléseket vagy információkat olyan helyszínekre, ahol a hagyományos közlekedési módok nem állnak rendelkezésre, továbbá elősegítheti az ipari katasztrófák következményeinek felderítését, felmérését, monitorozását, visszamaradó hatásának folyamatos nyomon követését. Kettős navigációs rendszere, mint a GPS és a tehetetlenségi navigációs rendszer (*inertial navigation system,* INS) kiegészítik egymást.

[19] Schiebel Aircraft [é. n.].

3. ábra: Schiebel M100 Camcopter
Forrás: a szerzők felvétele

Katonai alkalmazását tekintve képes adatokat gyűjteni és felderíteni harcászati körülmények között. A CBRN SaaS projekt keretében elsődleges célként fogalmazódott meg olyan függesztmény fejlesztése, amely képes különböző mérgező harcanyagok, valamint ipari toxikus anyagok detektálására és azonosítására levegőben. Ezenfelül integrálható az eszközre a Gamma Zrt. által fejlesztett radiológiai detektor, amellyel a rendszer valós időben képes adatokat közölni a radioaktív szennyezett terepszakaszról.

A drón sokoldalúsága lehetővé teszi alkalmazását katonai és civil felhasználási területeken is. Minél szélesebb spektrumú a felhasználási lehetősége egy költséges rendszernek, annál költséghatékonyabbnak nevezhető.

A hibrid meghajtás és az alacsony üzemanyag-fogyasztás lehetővé teszi, hogy a drón akár 6 órán keresztül is repüljön, míg más, hasonló eszközök esetén szükség lehet a feladat közbeni utántöltésre. Az eszköz képes működni extrém időjárási körülmények között is, például erős szélben vagy esőben, továbbá extrém hőmérsékleti körülmények között is képes feladatot végrehajtani.

Negatívum, hogy a magas fejlesztési és gyártási költségek miatt a drón beszerzése és üzemeltetése is drága lehet. Ezen túl, a drón kezeléséhez és karbantartásához magasan képzett szakemberek szükségesek, ami korlátozhatja a használhatóságát azokon a területeken, ahol nincsenek megfelelően képzett operátorok.

OneDrone SUAS

A szlovén OneDrone cég által gyártott VTOL szintén a rendszer részét képezi a kis méretű drón kategóriában. A platform fejlesztéséről a gyártó nyílt információkat nem tesz közzé. Mindezen túl, a SUAS egy merev szárnyú, helyből fel- és leszállásra képes kis méretű drón, amely a hozzá fejlesztett detektordokkoló egységgel *(sensor pod)* képes a szennyezett területre berepülni, és landolást követően a vegyi szennyezést mérni és detektálni.

A OneDrone SUAS nagy fokú vízállósággal rendelkezik, ami alkalmassá teszi ABV-szennyezett környezetben való tevékenységre, valamint folyami alkalmazásra egyaránt. Könnyű, jól szállítható, az össztömege a 25 kg-ot nem haladja meg. A szárnyfesztáv 3 m. Képes helyből fel-, leszállásra, valamint előre programozott útvonalak lerepülésére.[20]

A merev szárnyú drónok lehetővé teszik a gyors kijutást a mérési helyszínre, azonban a pontos mérések érdekében a sebességet csökkenteni szükséges. A VTOL-rendszerek kiküszöbölik a sebességből adódó pontatlanságot, azonban a vertikális mozgást, lebegést lehetővé tevő rotorok vegyi mérés esetén mérést zavaró turbulenciát okoznak, így a detektort a turbulencia árnyékzónájában kell elhelyezni.

DOK-ING UGS

A horvát DOK-ING-rendszer hibrid hajtóművel felszerelt, alkalmas szélsőséges körülmények közötti (például alacsony oxigénszint, magas hőmérséklet) feladat-végrehajtásra. Az integrált ABV-detektorokkal képes mérgező harcanyagok és veszélyes ipari anyagok detektálására, távdetektálására, sugárfelderítésre, emellett a működtetést támogató videórendszerrel is rendelkezik. Mintavevő karral, mintatároló rendszerével ambicionált az ABV-mintavétel gáz-, folyadék- és szilárd halmazállapotú mintákból, de a projekt első fázisának végén a folyadék-mintavétel még nem volt kiforrott, mivel az egy irányból képet adó kamerával az operátor nem érzékelhette megfelelően a térbeli mélységet, a mintavevő fej helyzetét. Az eszköz a 4. ábrán látható.

4. ábra: DOK-ING ABV-felderítő UGS
Forrás: a szerzők felvétele

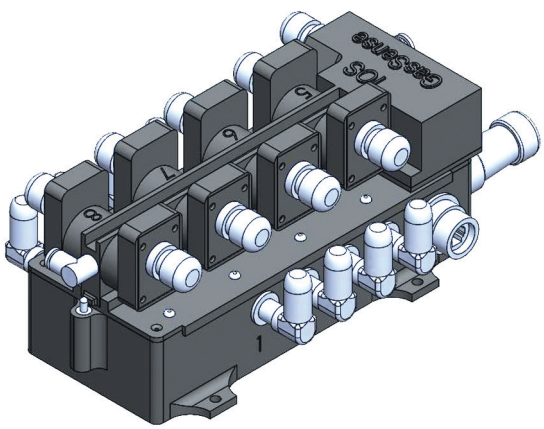
[20] Hofstätter 2024.

Az eszköz előnye, hogy pontos mérésekre képes, azonban nehézkes kezelése rendkívül lelassítja a felderítést, valamint súlyából adódóan körülményes a szállítása, emellett feltételezhetően a beszerzése is jelentős összeget követel majd meg.

Kulcsfontosságú részelemek

Detektordokkoló egység

A drónokhoz fejlesztett detektordokkoló egység különböző vegyi és sugárzásmérő detektorokat képes magában foglalni cserélhető módon. Az eszközzel szembeni egyik kritikus követelmény a minél kompaktabb kialakítás a drónok teherbírásához igazítva. A 5. ábrán modellezett eszköz egy időben 8 különböző vegyi anyag mérésére és detektálására képes, moduláris felépítéséből adódóan a szenzorok könnyen cserélhetők, variálhatók, továbbá a mérések során a valós mérési adatok a hőmérsékleti körülményekhez igazíthatók. A rendszer automatikus önellenőrzésre képes a hiteles mérési eredmények érdekében, Ethernet kommunikációval rendelkezik.



5. ábra: Detektordokkoló egység 3D-modellje
Forrás: Hofstätter 2024

Detektorok

Az alkalmazott vegyi szenzor a Gamma Zrt. által fejlesztett intelligens gázdetektor, amely képes foszgén, halogének (bróm, klór, fluor), arzén, kén-dioxid, kén-hidrogén, továbbá illékony szerves vegyületek detektálására. Az intelligens gázdetektor a 6. ábrán látható. Az intelligens gázdetektorok egyik legfontosabb megkülönböztető jegye a modularitás és a távvezérelt működtetés lehetősége. A hagyományos kézi vegyi detektorok elsődleges előnye a gyors telepíthetőség és a közvetlen visszajelzés, ugyanakkor alkalmazásuk jelentős kockázatot jelent ABV-szennyezett környezetben.

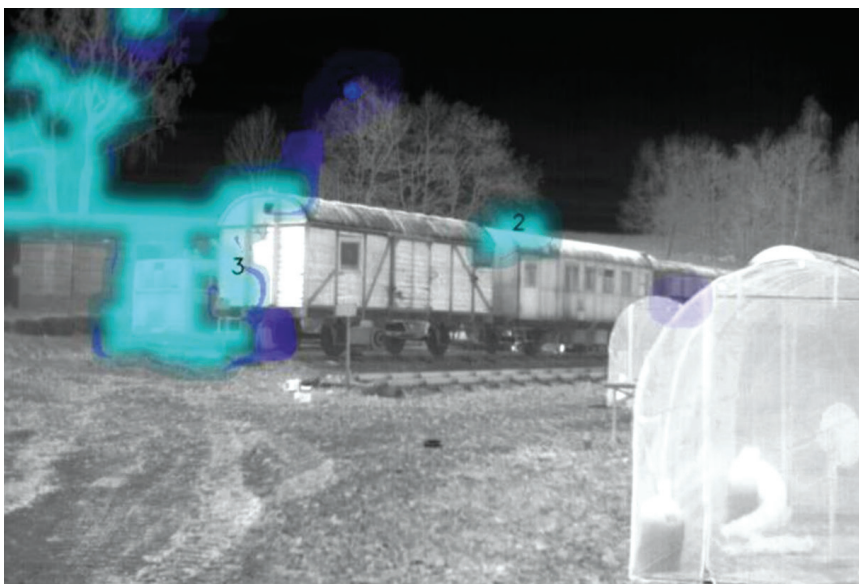
A pilóta nélküli platformokra integrált detektorok lehetővé teszik a szennyezett terület fizikai megközelítése nélküli mérést, a mérési adatok valós idejű továbbítását, valamint a mérések ismételhetőségét előre meghatározott útvonalak mentén.

6. ábra: Intelligens gázdetektor
Forrás: GTI SGM, GAMMA Zrt. [é. n.]

A radiológiai szennyezés detektálásáért szintén a Gamma Zrt. által fejlesztett Geiger–Müller típusú detektor, valamint egy nagy érzékenységű szcintillációs elven működő detektor felel, amely képes radioaktív izotópok azonosítására. Közvetlenül kapcsolódnak a CE–CCE–DFC-architektúrához, lehetővé teszik a sugárszint térbeli leképezését, és támogatják a több forrásból származó adatok együttes értékelését. Ez a megközelítés különösen előnyös olyan műveleti környezetben, ahol a sugárszennyezés kiterjedése és intenzitása gyorsan változik, és a döntéshozatalhoz nem önálló mérési pontokra, hanem összefüggő helyzetképre van szükség.

7. ábra: Second Sight MS távdetektor
Forrás: Hofstätter 2024

A Bertin cég által fejlesztett Second Sight MS távdetektor a 7. ábrán látható módon a DOK-ING UGV-re integrált, a vegyi távdetektálási képesség érdekében. Az eszköz 5 km távolságból is képes detektálni a mérgező harcanyagok, valamint a veszélyes ipari anyagok jelenlétét multispektrális infravörös képalkotó rendszer segítségével. A 8. ábra bemutatja az eszköz által készített hőképet. Az eszköz alapvetően nagy mennyiségű kibocsátást képes detektálni, azonosításra azonban nem alkalmas.



8. ábra: A távdetektor hőképe a teszt során
Forrás: Hofstätter: 2024

A tesztek tapasztalatai

Az EDA CBRN SaaS projekt két fázisra tagozódott. Az első fázis végéig, azaz 2024. május 31-ig, az ipari konzorciumnak el kellett érnie a műszaki követelményeknek megfelelő, úgynevezett technológiai demonstrátorok kifejlesztését. Az időrend tartása és a források ütemezett kifizetése érdekében a tagországok képviselői, illetve az EDA projektmenedzsere részére az AIT vezetője félévente beszámolt az időarányos részcélkitűzések teljesítéséről. A követelmények teljesítése érdekében a CBRN SaaS keretében a tagállamok által megszervezve, az ipari konzorcium tagjainak együttműködésével több terepi tesztre is sor került. Az első tesztnek 2023. október 15–20. között Magyarország adott otthont a Magyar Honvédség Böszörményi Géza Csapatgyakorlótér Kiképző Bázisán Újdörögdön és a környező gyakorlótéren, amely során a résztvevők a biológiai mintavételt tesztelhették, de gyakorlatilag ez az első olyan alkalom volt, amikor együtt dolgozhattak a teljes ipari konzorcium cégeinek szakértői, illetve a projekttagországok képviselői.

A radiológiai, sugárfelderítés tesztelésére 2023. november 13–17. között Szlovéniában került sor, majd 2024. március 11–15. között Horvátországban a vegyi felderítés, mintavétel, valamint az eszközök ABV-mentesítésének tesztelését hajtották végre. Az első fázis zárásaként a teljes rendszer vizsgálata 2024 áprilisában volt Ausztriában. A teszteket követő bemutatókra az EDA meghívta a projektben részt vevő országok katonai vezetőit, hadfelszerelési, továbbá képeségfejlesztési igazgatóit. A DV-napon a magyar delegációt Somogyi Zoltán vezérőrnagy, HVK törzsigazgató vezette.

Az első fázis során pozitív tapasztalat volt az EDA-projekt folyamatos fejlődése. A projektmenedzser szorosan együttműködött a részt vevő nemzetek képviselőivel, továbbá az ipari konzorcium vezetőivel, amely során a kidolgozandó, fejlesztendő dokumentumokat, eszközöket, a projekt kezdetén jóváhagyott ütemterv figyelembevételével folyamatosan követte. A technológiai demonstrátorok kifejlesztését a terveknek megfelelően az első fázis végéig a konzorcium megvalósította. További pozitívum Ausztria mint vezető nemzet elhivatottsága mind az anyagi hozzájárulás, mind a feladatok vállalása tekintetében.

A technológiai demonstrátorok kifejlesztésével az első fázis végére a projekt elérte a kezdeti műveleti képességet.

A projekt második fázisának első felében a célkitűzés a technológiai demonstrátorok alkalmassá tétele katonai alkalmazásra. 2025-ben folytatódott a rendszer elemeinek tesztelése külön-külön és integrálva egyaránt. Az egyik fontos tesztelési fázis 2025 októberében volt, ahol az adattovábbítást és a szenzor dokkoló egységét vizsgálták. A vizsgálat fő célja az volt, hogy kiderítsék, a *sensor pod* képes-e mozgás közben is megbízhatóan, érezhető késleltetés nélkül továbbítani a mérési adatokat a CE, illetve a CCE felé. A teszt során vizsgálták a kapcsolat stabilitását, a tényleges átviteli sebességet, és hogy mennyire kritikus az adatok előzetes tömörítése (adatredukció).

Annak érdekében, hogy a külső környezeti zajok ne zavarják össze az eredményeket, egy előre összeállított szimulációs adatfolyamot használtak. A teszt során a *sensor podot* egy drónra szerelték, amely előre beprogramozott útvonalat repült be, miközben folyamatosan kommunikált a földi vezérlőegységgel. A teszt alatt a *sensor pod* és a vezérlőegység között 2–3 km-es távolságot tartottak, végig biztosítva a közvetlen rálátást (*line of sight,* LOS). Az adatkapcsolatot a Bonn Hungary Kft. TCP/IP-alapú MIMO rádiói adták. A folyamat során végig monitorozták a jelerősséget, a sávszélességet és az esetleges csomagvesztéseket. A továbbított adatcsomag leképezte a valódi szenzoradatok mennyiségét és szerkezetét. A mérések azt mutatták, hogy a *sensor pod* és a CE között az adatátvitel stabilan a 20–50 Mbit/s közötti tartományban maradt, amely sebesség elegendő a CBRN SaaS-rendszer alapkövetelményeihez, amelyek az ABV-helyzetkép kialakítását ambicionálják. A vizuális visszajelzés – azaz az élő videókép és a mérési adatok együttes továbbítása – zökkenőmentesen működött.

Az elemzés kvalitatív módszertannal történt, amely a detektorok műszaki paraméterei helyett azok funkcionális képességeit, modularitását, adatkezelési lehetőségeit és műveleti alkalmazhatóságát vizsgálta.

A fejlesztés és tesztelés jelenlegi szakaszában az egyik fő kihívás az adatmennyiség redukálás a CE–CCE–DFC között történő adatkommunikáció során. Az adatok továbbítása a detektor és a CE között (*Interface 1*) nem titkosított módon történik, azonban követelmény, hogy a CE–CCE–DFC (*Interface 2-3*) közötti adatkapcsolat

már titkosított legyen. Az adatredukció fontossága abban mutatkozik meg, hogy a rendszer képes legyen használható helyzetképet megjeleníteni a lehető legkisebb és legszükségesebb adatfelhasználás mellett. Az ehhez hasonló rendszereknél az egyik legnagyobb kihívást a digitális adattovábbítás minősége és mennyisége jelenti nagyobb távolságokra, ami megoldható hagyományos, új generációs digitális rádiótechnikai eszközökkel, VSAT- vagy egyéb műholdas adatátviteli rendszerrel, mint a Starlink. A tesztelés során a BHE Bonn Hungary Kft. által forgalmazott rádiók szolgáltatták az adatfolyamot az Interface 1 esetén, míg az Interface 2-3 esetén az Ausztriában rendszeresített adatkommunikációs eszközöket alkalmazták. Az eredmények igazolták, hogy a rendszer alkalmas a valós idejű adatcserére, feltéve, hogy nem a nyers, hanem az előfeldolgozott és tömörített adatokat mozgatjuk a hálózaton.

A drónok tekintetében nem prioritás azok további tesztelése, mivel ezek a platformok már megmérettettek a korábbi tesztek során, különböző időjárási körülmények között. A *sensor pod* esetében a detektorok mérési képességeit laborkörülmények között és terepen egyaránt folyamatosan tesztelik, és eredményességük az elvártaknak megfelelően alakul.

A jövőbeli tervek alapján Szlovéniában, Horvátországban és Magyarországon is végrehajtanak majd különböző teszteket a rendszer egyes elemeit és egészét illetően egyaránt. A rendszer teljes teszteléséhez egy workshop keretében olyan szcenáriókat alakítottak ki, amelyek segítségével tesztelhetővé válik különböző típusú feladatokban a rendszer alkalmassága és korlátai is. Ezek a szcenáriók alapvetően katonai műveletet, illetve különböző ipari katasztrófákat szimuláló helyzetet állítanak be.

Az ambicionált végállapot szerint a második fázis befejeztével elérhető és lekérhető a partnerországok számára egy olyan, Ausztriában települt többnemzeti alegység, amely a rendszer részelemeivel szolgáltatásként ABV-felderítést, -figyelést hajt végre és az adatokat a fogadó, azaz a megrendelő fél részére kezelhető, értékelhető módon adja át. A képesség kialakításának csak egy része a technikai eszközök megléte, a kezelők felkészítése, valamint az interoperabilitás megoldása. Az ambíciók teljesítéséhez a DOTMLPFI[21] alapján az összes képesség-összetevőt szükséges figyelembe venni, így a második fázis teljesítése érdekében Magyarország felajánlotta szakértők részvételét a doktrinális háttér kidolgozásához, valamint drónpilóta-kiképzők részvételét a drónok kezelése érdekében.

Összegzés

Tekintettel a digitalizálás célkitűzésére, az élőerő megóvására, valamint az általános és ezen belül az ABV-helyzetkép minél aprólékosabb, pontosabb meghatározásának igényére, a szenzorok harctéri alkalmazásának növelése, a vonatkozó innovációk támogatása kötelező érvényűnek tűnik. Az ABV-helyzetkép kialakítása elengedhetetlen a csapatok túlélőképességének és a manőver szabadságának fenntartásához

[21] *Doctrine, organization, training, material, leadership development, personnel, facilities, interoperability* azaz doktrína, szervezeti felépítés, kiképzés, anyagok és felszerelés, vezetői felkészítés, személyi állomány, infrastruktúra és interoperabilitás.

szennyezett környezetben, miközben lehetővé teszi a kockázatarányos döntéshozatalt, a védelmi rendszabályok pontos időzítését.

Az UGS/UAS-ek folyamatosan változnak, hogy megfeleljenek a technológiai fejlődés és a modern hadviselés egyre bonyolultabb igényeinek. A drónok alkalmazása megkerülhetetlen, különösen a távérzékelés, a logisztika és a katasztrófaelhárítás területén, miközben a fejlesztők továbbra is dolgoznak a drónok autonómiájának növelésén, hogy a jövőben még komplexebb feladatokat végezhessenek el emberi beavatkozás nélkül, miközben az eszközök nagyobb hatótávolsággal, hosszabb repülési idővel és nagyobb teherbírással is rendelkezzenek.

A Magyar Honvédség szerepvállalása, a többnemzeti alegységhez való hozzájárulás mértéke még nem eldöntött, azonban *kritikus fontosságú, hogy a CBRN SaaS-t rendszerek rendszerének tekintsük*. A CBRN SaaS-rendszerben alkalmazott eszközök (drónok, detektorok, szoftverek) legnagyobb hozzáadott értéke nem az egyedi műszaki paraméterekben, hanem a rendszerszintű integrációban és az adatfúzióban rejlik. A hazai, légi sugárfelderítési képesség fejlesztésére, annak alkalmazására vonatkozó kutatások, erőfeszítések huzamos ideje zajlanak, vonatkozó publikáció már található 2009-ből,[22] illetve 2025-ből is,[23] azonban ezek összehasonlítása az EDA-projekttel több okból sem célszerű: egyrészt a többnemzeti fejlesztés nem helikopterekre, hanem UGS/UAS-platformokra koncentrál, másrészt a sugárfelderítésen túl vegyi felderítés és ABV-mintavétel is ambicionált, harmadrészt az EDA-projekt rendszerének csak egy része a felderítést végrehajtó eszközök és detektorok, *a Magyar Honvédség részére valódi potenciált a adatforgalom és az adatokat kezelő szoftverek felhasználása, adaptálása jelentheti.* A fejlesztés nem pusztán három drónt tartalmaz, hanem a drónokra integrálható detektorokat, az adattovábbító rendszert, valamint az adatok feldolgozására alkalmas szoftvereket is. A részelemek különválaszthatók, a drónok tekinthetők csupán a detektorokat szállító platformnak is. Nem feltétlenül előremutató nagyon sok, egymástól gyökeresen eltérő dróntípussal dolgozni Magyar Honvédség szinten mind a logisztikai háttér, mind az eltérő igényű kezelői képzések miatt, és a CBRN SaaS projekt nem is feltétlenül követeli meg újabb drónok rendszeresítését. A fejlesztésben részt vevő magyar cégek szakterülete felhasználói szemmel tekintve rendkívül szerencsés. Magyar cég felel a detektorok fejlesztéséért, valamint szintén magyar cég felelős az adatok továbbításáért, ami azt jelenti, hogy a hordozó platformok cseréjének alapvető feltételeivel Magyarország rendelkezik. A fejlesztő cég képviselőjének állásfoglalása alapján a DFC szoftvere a rendszerből kikülöníthető, egyéni igények szerint módosítható, így a Magyar Honvédség saját drónokkal is képes lehet azt használni, továbbá a DFC beszerzését követően az felajánlható az ambicionált többnemzeti alegység működéséhez is.

[22] Zelenák et al. 2009.
[23] Mészáros 2025.

Felhasznált irodalom

BHE (2024): *European Defence Agency's CBRN SaaS Project Achievements.* Online: https://bhe-corp.com/european-defence-agencys-cbrn-saas-project-achivements/

Binding Commitments [é. n.]. Online: www.pesco.europa.eu/binding-commitments/

European Commission (2016): *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign and Security Policy* [ePub], June 2016. Online: www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

European Commission (2021): *CBRN RSS Chemical, Biological, Radiological and Nuclear Reconnaissance and Surveillance System*. Online: https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP2020_factsheet_CBRN__DEWS_CBRN-RSS.pdf

European Commission [é. n.]: *European Defence Industrial Development Programme (EDIDP).* Online: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en

European Defence Agency (2010): *General Rules and Procedures Applicable to Ad Hoc Research & Technology Projects and Programmes of The European Defence Agency.* Online: https://eda.europa.eu/docs/documents/EDA_General_Rules_and_Procedures.pdf

European Defence Agency (2023): *The 2023 EU Capability Development Priorities.* Online: https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf

Európai Unió (2008): Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata – JEGYZŐKÖNYVEK – (10.) Jegyzőkönyv: az Európai Unióról szóló szerződés 42. cikkével létrehozott állandó strukturált együttműködésről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12008M/PRO/10.

GTI-SGM (-EX) Gas Detector Family [é. n.]. Online: www.gammatech.hu/index.php?mnuGrp=mnuProducts-mnuProducts_Category&module=products&-lang=eng&group=kornyezetimonitoring_gas&product=gtisgmex&menupath=-main-kornyezetimonitoring-kornyezetimonitoring_gas-

HOFSTÄTTER, Michael (2024): *CBRN SAAS (EDA CAT. B.) Chemical, Biological, Radiological and Nuclear Reconnaissance and Surveillance System – Technological Demonstrator.* Austrian Institute of Technology GmbH, MS Powerpoint előadás, 2025. június 16. EDA CBRN SaaS PAMG értekezlet, Bécs.

MCMANUS, Keith David (2019): *Radiological and Nuclear Threat Detection Using Small Unmanned Aerial Systems.* Berkeley: University of California. Online: https://escholarship.org/uc/item/7b241431

MÉSZÁROS Zalán (2025): Az LSF–21 légi sugárfelderítő konténer fejlesztése. *Haditechnika,* 59(3), 44–51. Online: https://real.mtak.hu/226668/1/PagesfromHT_2025_3_book_netre-9.pdf

MOLNÁR Anna – SZABOLCS Laura (2020): Megerősített együttműködés, változó geometria, PESCO. *Hadtudomány,* 30(4), 77–106. Online: https://doi.org/10.17047/Hadtud.2020.30.4.77

Pavlovsky, Ryan et al. (2018): *3-D Radiation Mapping in Real-Time with the Localization and Mapping Platform LAMP from Unmanned Aerial Systems and Man-Portable Configurations. ArXiv.* Online: https://doi.org/10.48550/arXiv.1901.05038
Pusch, Gunther (2021): *CBRN SaaS Project Enters Operational Phase.* EDA. Online: https://eda.europa.eu/news-and-events/news/2021/01/21/cbrn-saas-project-enters-operational-phase
Schiebel Aircraft GmbH [é. n.]: *Camcopter® S100.* Online: https://schiebel.net/s-100-brochure/
Zelenák János et al. (2009): A légi sugárfelderítés képességei alkalmazhatóságának vizsgálata elveszett, vagy ellopott sugárforrások felkutatása, illetve szennyezett terepszakaszok felderítése során. *Hadmérnök,* 4(1), 46–62. Online: http://hadmernok.hu/2009_1_zelenak.pdf

Jogi források

Consolidated Version of The Treaty on European Union. Online: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF
Council Decision (CFSP) 2017/2315 of 11 December 2017 Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States. Online: https://eur-lex.europa.eu/eli/dec/2017/2315/oj/eng

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 1. szám 125–135.
DOI: 10.32567/hm.2026.1.8

Kocsis Zoltán,[1] Vass Gyula[2]

A kritikus szervezetek rezilienciája különös tekintettel az EU–USA szabályozási keretek összehasonlítására

The Resilience of Critical Organisations with Special Emphasis on the Comparative Analysis of EU and US Regulatory Frameworks

Absztrakt

A kritikus szervezetek rezilienciája az elmúlt évtizedben a katasztrófavédelem, a közigazgatás és a nemzetbiztonság egyik központi kérdésévé vált. A tanulmány célja annak bemutatása és összehasonlító elemzése, hogy az Európai Unió (EU) és az Amerikai Egyesült Államok (USA) milyen szabályozási és intézményi megközelítéseket alkalmaz a kritikus szervezetek ellenálló képességének erősítésére. Jelen cikkben a szerzők áttekintik a reziliencia fogalmát és jelentőségét a társadalmi és gazdasági folyamatok, a környezet és a védelmi képességek stabil fenntartásában, valamint a lakossági alapvető szolgáltatások biztonsága szempontjából. Ezt követően részletesen összehasonlítják az Európai Unió és az Amerikai Egyesült Államok jogi és stratégiai szabályozási kereteit a kritikus infrastruktúrák és szervezetek rezilienciájának, azaz ellenálló képességének erősítése terén. A tanulmány rámutat, hogy míg mindkét térségben növekvő hangsúlyt kap az összveszély megközelítésű reziliencia a természeti katasztrófák, járványok és egyéb krízisek kezelésében, addig az EU szabályozása inkább jogilag kötelező erejű irányelvekkel és átfogó stratégiákkal igyekszik növelni a létfontosságú szolgáltatást nyújtó entitások ellenálló képességét, míg az USA szabályozása hosszú ideig önkéntes

[1] Iparbiztonsági szakértő; tulajdonos, ECIP Kft.; oktató, Pannon Egyetem Mérnöki Kar Fenntarthatósági Megoldások Kutatólaboratórium, e-mail: kocsis.zoltan@ecip.hu
[2] Tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Műszaki Tanszék, e-mail: vass.gyula@uni-nke.hu

együttműködésre és irányelvekre épített, amelyet a legújabb stratégiák már kötelezőbb elemekkel egészítenek ki. A tanulmány megállapítja, hogy a két megközelítés fokozatos közeledése egy hibrid rezilienciamodell irányába mutat, amely releváns tanulságokkal szolgál a közigazgatás és a katasztrófavédelem fejlesztése számára.

Kulcsszavak: reziliencia, kritikus szervezetek, közigazgatás, ellátásbiztonság, Európai Unió, Amerikai Egyesült Államok

Abstract

The resilience of critical organisations has become a key issue in disaster management, public administration, and national security over the past decade. The aim of this study is to provide a comparative analysis of the regulatory and institutional approaches adopted by the European Union (EU) and the United States of America (USA) to strengthen the resilience of critical organisations. In this article, the authors review the concept of resilience and its significance in the stable maintenance of social and economic processes, the environment and defence capabilities, and the security of essential services for the population. This is followed by a detailed comparison of the legal and strategic regulatory frameworks of the European Union and the United States of America in terms of strengthening the resilience of critical infrastructures and organisations. The study shows that while both regions are increasingly focusing on all-hazards resilience in managing natural disasters, epidemics and other crises, EU regulation tends to focus on legally binding guidelines and comprehensive strategies to increase the resilience of entities providing essential services, while USA regulation has long been based on voluntary cooperation and guidelines, which are supplemented by more mandatory elements in recent strategies. The study concludes that the gradual convergence of these approaches points toward a hybrid model of resilience, offering valuable lessons for the development of public administration and disaster management.

Keywords: resilience, critical organisations, public administration, security of supply, European Union, United States of America

Bevezetés

A modern társadalmak egyre összetettebb kihívásokkal néznek szembe, ideértve a természeti katasztrófákat, pandémiákat, gazdasági válságokat és akár szándékos támadásokat is. E kihívások közepette kulcsfontosságú, hogy a kritikus szervezetek reziliensek legyenek, beleértve a közszféra intézményeit és az alapvető szolgáltatásokat nyújtó infrastruktúrákat, azaz képesek legyenek a váratlan eseményeket kezelni és működésüket gyorsan helyreállítani. A reziliencia fogalma eredetileg az ökológiában jelent meg, de mára interdiszciplináris megközelítésben alkalmazzák a kormányzás és válságkezelés területén is.[3]

[3] Pálné Kovács 2023.

A Covid–19-járvány különösen ráirányította a figyelmet az ellenálló képességre építő szakpolitikák fontosságára, hiszen világossá vált, hogy a közigazgatási és a gazdasági szereplők felkészültsége és alkalmazkodóképessége alapvetően befolyásolja a válságkezelés sikerét. Ennek nyomán mind globális, mind nemzeti és helyi szinten kihívásként jelent meg a reziliencia intézményesítése a közigazgatásban és a létfontosságú szolgáltatások biztosításában.

A bevezető célja, hogy meghatározza a reziliencia, azaz az ellenálló képesség fogalmát, és keretet adjon a későbbi elemzésnek. A rezilienciát általánosan egy rendszer azon kapacitásaként definiálják, hogy képes megbirkózni a külső sokkokkal, alkalmazkodni a változásokhoz, és megőrizni alapvető struktúráit és funkcióit.[4] Ez nem pusztán a „visszapattanást" jelenti a kiinduló állapotba, hanem gyakran „előre pattanást" is. A rendszer tanul a krízisből és akár egy új, jobb egyensúlyi állapotba fejlődik tovább. A közigazgatásban a reziliencia fogalma sok tekintetben szembemegy a hagyományos bürokratikus jellemzőkkel, a merev hierarchiával és szabályorientáltsággal, és rugalmasabb, adaptívabb működésmódot követel meg a váratlan helyzetek kezelésére.[5]

A reziliencia fogalma az elmúlt évtizedekben több tudományterületen is megjelent, eltérő értelmezési keretek között. Eredetileg az ökológia és a pszichológia területén használták, ahol a rendszerek és egyének alkalmazkodóképességét, illetve a sokkhatások utáni helyreállítás képességét írta le.[6] A biztonságpolitika és a közigazgatás területén a reziliencia ennél összetettebb jelentéstartalmú, mivel nem csupán a helyreállítás, hanem a megelőzés, az alkalmazkodás és az átalakulás képességét is magában foglalja.[7]

A szakirodalom a rezilienciát gyakran négy alapvető dimenzió mentén értelmezi: ellenállás, alkalmazkodás, helyreállítás és tanulás. E megközelítés szerint a reziliens rendszer nemcsak túléli a válsághelyzeteket, hanem képes azokból tanulságokat levonni, és működését ennek megfelelően módosítani. A kritikus szervezetek esetében ez különösen fontos, mivel működésük zavara közvetlen hatással van a társadalom alapvető funkcióira. A közigazgatási és biztonságpolitikai értelmezésekben a reziliencia egyre inkább kormányzási paradigmává válik.[8] Nem kizárólag technikai védelemként jelenik meg, hanem olyan szervezeti és intézményi képességként, amely a komplex és kiszámíthatatlan kockázati környezethez való alkalmazkodást segíti elő. A reziliencia e felfogásban nem helyettesíti a klasszikus védelemfogalmakat, hanem kiegészíti azokat, hangsúlyt helyezve a rugalmasságra és a hálózatos együttműködésre.[9]

A szerzők által alkalmazott kutatási módszertan kvalitatív módszertanon alapul, dokumentumelemzés és összehasonlító szakpolitikai elemzés alkalmazásával. Jelen cikk a reziliencia jelentőségét tárgyalja a közigazgatásban és a gazdasági szereplők működésében, különös tekintettel arra, miként járul hozzá a lakosság alapvető ellátásbiztonságához és a katasztrófavédelmi felkészültséghez. Ezt követően a szerzők

[4] Gunderson 2010.
[5] Profiroiu–Nastacă 2021.
[6] Székely 2015.
[7] Kádár–Keszely 2025.
[8] Mógor – Baloghné Pruha 2025.
[9] Ambrusz–Vásárhelyi 2025.

összehasonlítják az Európai Unió és az Amerikai Egyesült Államok szabályozási kereteit e területen, rávilágítva a megközelítésbeli különbségekre és hasonlóságokra.

A reziliencia jelentősége a közigazgatásban, önkormányzatokban és ellátásbiztonságban

A közigazgatási intézmények rezilienciája kulcsfontosságú a társadalom egésze szempontjából, mivel a kormányzati szerveknek válsághelyzetek idején is biztosítaniuk kell az alapvető közszolgáltatásokat és a rend fenntartását.[10] Rámutatnak, hogy a közintézményeknek erősíteniük kell képességeiket a rendkívüli események kezelésére, vagyis a különféle külső és belső váratlan hatásokkal szemben ellenállóvá kell válniuk. Ez magában foglalja a kockázatok folyamatos értékelését, vészhelyzeti tervek kidolgozását, a személyzet képzését és a szervezeti rugalmasság fejlesztését. Az intézményi reziliencia növelése azért létfontosságú, mert a merev, centralizált rendszerek nehezebben reagálnak gyorsan a krízisekre, míg a tanuló szervezetek és a hálózatos együttműködések hatékonyabbak a válságok során. Empirikus tapasztalat, hogy a kormányzatok minősége és felkészültsége nagymértékben hozzájárul a válságok sikeres kezeléséhez vagy kudarcához. A krízisekre való felkészülést ezért rendszerszinten be kell építeni a kormányzati működésbe. Így elkerülhető, hogy vészhelyzetben kizárólag improvizatív, rendkívüli eszközökre kelljen támaszkodni. Önkormányzati szinten a reziliencia még közvetlenebb módon érződik a lakosság mindennapi biztonságában. A települési önkormányzatok felelnek számos alapvető közszolgáltatásért, mint az ivóvíz, helyi közlekedés, hulladékkezelés, alapegészségügyi ellátás vagy a közbiztonság, ezért válsághelyzetben elsődleges, hogy e szolgáltatások fenntartása biztosítva legyen. A 2020–2021-es pandémiás tapasztalatok rámutattak, hogy ahol az önkormányzatok megfelelő autonómiával, erőforrásokkal és krízistervekkel rendelkeztek, ott a helyi közösségek jobban átvészelték a járványt, míg a centralizációs intézkedések és az erőforráshiány sok helyen gátolták a hatékony reagálást.[11] Az önkormányzati ellenálló képesség fejlesztése ezért kiterjed a helyi szintű kockázatértékelésre, a közösségi tervezésre és a civil szektor bevonására is a vészhelyzeti előkészületekbe.

A közigazgatási intézmények rezilienciája ennek megfelelően a modern állam működőképességének egyik alapfeltétele. Válsághelyzetek idején – legyen szó természeti katasztrófáról, járványról vagy technológiai eredetű zavarokról – a közigazgatás feladata nem csupán a rend fenntartása, hanem az alapvető közszolgáltatások folytonosságának biztosítása is. A reziliens közigazgatás ezért olyan intézményi és szervezeti képességekkel rendelkezik, amelyek lehetővé teszik a gyors döntéshozatalt, az erőforrások rugalmas átcsoportosítását és a hatékony koordinációt.

Végül, a reziliencia kritikus a lakosság ellátásbiztonsága szempontjából is. Ide tartozik mindazon kritikus infrastruktúrák és alapvető szolgáltatások köre, mint az energiaellátás, ivóvíz- és élelmiszer-ellátás, az egészségügyi rendszer, pénzügyi szolgáltatások, hírközlés, közlekedés stabil működtetése, amelyek nélkül a mindennapi

[10] Profiroiu–Nastacă 2021.
[11] Pálné Kovács 2023.

élet megbénulna. Az Európai Bizottság megfogalmazása szerint „megbízható energiaellátás, biztonságos ivóvíz, egészségügyi szolgáltatások, banki és pénzügyi szolgáltatások, infokommunikációs szolgáltatások, valamint kiszámítható közlekedés nélkül modern életformánk lehetetlen lenne", ezért a kritikus infrastruktúrák védelme és a kritikus entitások rezilienciája alapvető a társadalom számára. Ebben a relációban kiemelt szerepe van a kibertér védelmének, amely tovább erősíti azt, hogy a kritikus infrastruktúrákon belüli kiberbiztonság megvalósítása elemi érdeke kell hogy legyen minden infrastruktúra-tulajdonosnak és üzemeltetőnek.[12]

A lakossági ellátásbiztonság rezilienciája azt jelenti, hogy e rendszerek képesek ellenállni a természeti katasztrófáknak (árvíz, földrengés, viharkárok), a technológiai meghibásodásoknak (hálózati üzemzavarok), az emberi eredetű fenyegetéseknek (terrorizmus, kibertámadás), valamint esetleges szolgáltatáskimaradást követően gyorsan helyre tudnak állni. Az ellátásbiztonság érdekében kulcsfontosságú a kockázatok azonosítása, elemzése és értékelése, a katasztrófavédelmi tervezés és gyakorlatok végzése, a redundáns kapacitások kialakítása (tartalék rendszerek, alternatív ellátási útvonalak), valamint a lakosság tájékoztatása és bevonása az önvédelmi képességek fejlesztésébe. Összességében tehát a reziliencia elősegíti, hogy a kritikus szervezetek és infrastruktúrák a lehető legkisebb fennakadással vészeljék át a krízíseket, biztosítva ezzel a közszolgáltatások folytonosságát, a társadalmi és gazdasági folyamatok fenntartását.

A közigazgatás és az ellátásbiztonság rezilienciájának erősítése ezért olyan átfogó megközelítést feltételez, amely integrálja a jogi szabályozást, az intézményi kapacitásfejlesztést és a társadalmi együttműködést. E komplex szemlélet képezi azt a keretet, amelyben értelmezhető az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási rendszereinek összehasonlítása. Az összehasonlító elemzés részletes eredményeit a következő fejezet mutatja be.

Az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási kereteinek összehasonlítása

Az Európai Unió megközelítése

Az EU-ban az elmúlt két évtizedben fokozatosan épült ki a kritikus infrastruktúrák védelmének és rezilienciájának átfogó keretrendszere. Kezdetben a hangsúly a kritikus infrastruktúrák védelmén volt (*critical infrastructure protection,* CIP), különösen a 2000-es években meghozott 2008/114/EK irányelvben, amely az európai kritikus infrastruktúrák azonosítását, kijelölését és védelmét célozta meg főként az energia- és közlekedési ágazatban.[13] Az utóbbi években azonban az EU stratégiája jelentős paradigmaváltáson ment keresztül, áthelyezve a hangsúlyt a védelemről a reziliencia növelésére.[14] E szemléletváltást tükrözi az új, 2022-ben elfogadott kritikus entitások

[12] Kovács 2018a.
[13] European Commission 2026.
[14] Tierney 2015.

rezilienciájáról szóló irányelv *(Directive on the Resilience of Critical Entities, 2022/2557 EU Directive),* amely 2023 januárjában lépett hatályba.[15]

Az új szabályozás olyan összveszély *(all-hazards)* megközelítést alkalmaz, amely nemcsak a terrorcselekmények vagy szándékos károkozás ellen kíván védelmet nyújtani, hanem a természeti veszélyek, járványok, káresemények és egyéb fenyegetések ellen is erősíti az alapvető szolgáltatásokat nyújtó szervezetek ellenálló képességét.

Az irányelv előírja, hogy a tagállamok fogadjanak el nemzeti stratégiát a kritikus entitások rezilienciájára, és rendszeresen végezzenek nemzeti kockázatértékelést, amelyek alapján az ellenálló képesség fokozására stratégiai célkitűzéseket és prioritásokat állapítsanak meg, valamint támogassák a kritikus szervezetek kockázatértékelését és ezáltal az ellenálló képességi intézkedéseit.

Az Európai Bizottság közös uniós alapvető szolgáltatás lista alapján segíti ezt a munkát, amely meghatározza az érintett ágazatokat és szolgáltatásokat. Az irányelv tizenegy kulcságazatot sorol fel, köztük az energiát, a közlekedést, a banki szolgáltatásokat, a pénzügyi piaci infrastruktúrát, az egészségügyet, az ivóvíz- és szennyvízszolgáltatást, a digitális infrastruktúrát, az élelmiszer-ellátást, valamint a közigazgatást és az űrinfrastruktúrát is. Újdonság, hogy a „kritikus entitás" fogalma alá már nemcsak a hagyományos értelemben vett infrastrukturális üzemeltetők tartoznak, hanem például állami hivatalok vagy kulcsfontosságú hatóságok is, vagyis minden olyan szervezet, amely nélkülözhetetlen a társadalom és gazdaság működéséhez.[16] A kritikus entitásoknak saját kockázatelemzést kell készíteniük, és megfelelő technikai, fizikai és szervezési intézkedéseket kell bevezetniük a rezilienciájuk fokozása érdekében, beleértve az ellenálló képességi tervek készítését és az incidensek bejelentését a hatóságok felé. A tagállamok kötelesek támogatást nyújtani e szervezeteknek (például képzések, útmutatók, pénzügyi támogatások formájában), míg az Európai Bizottság uniós szinten összehangolja az információcserét, bevált gyakorlatok megosztását, közös kockázatelemzést és akár határokon átnyúló szimulációs gyakorlatokat is szervez. Fontos eleme a keretnek a tagállamok közötti és uniós szintű koordináció, amelynek érdekében hozták létre a Kritikus Entitások Rugalmassági Csoportját (Critical Entities Resilience Group, CERG), amely biztosítja a nemzeti hatóságok képviselőinek és az európai bizottsági szakértőknek az együttműködését. Emellett válaszul az utóbbi évek kritikus infrastruktúrák elleni incidenseire (például gázvezeték-szabotázs), 2022 végén az EU Tanácsa ajánlást fogadott el a tagállamok reziliencianövelő intézkedéseinek összehangolt erősítésére, külön hangsúlyt fektetve a megelőzésre, felkészülésre és reagálásra.

Az Európai Unió a kiberbiztonsági stratégiájában olyan holisztikus megközelítést alkalmaz, amely jóval túlmutat a kibertéren, hiszen az olyan kapcsolódó területek biztonságának növelését is célul tűzte ki, mint a kritikus infrastruktúrák területe. Az ellenálló képesség terén a stratégia kiemeli a kiberbiztonsági tudatosság fejlesztését, amelyben a felhasználók internetes tevékenységeinek minél nagyobb biztonságát hangsúlyozza.[17]

[15] Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.

[16] Lazari 2022.

[17] Kovács 2018a.

Összességében az EU megközelítését a szabályozási minimumkövetelmények és a jogilag kötelező erejű keretek jellemzik. Az uniós tagállamok számára előírás, hogy a kritikus ágazatokban működő entitásokkal szemben bizonyos biztonsági és üzletmenet-folytonossági követelményeket támasszanak, és ezeket a nemzeti jogba átültetve betartassák. Ugyanakkor az EU felismeri a tagállami szuverenitás és felelősség szerepét, így a keretrendszer rugalmasan alkalmazható a nemzeti sajátosságokhoz, de egy közös minimumszintet garantál a teljes Unió területén.

Az Amerikai Egyesült Államok megközelítése

Az Egyesült Államokban a kritikus infrastruktúrák védelmének és rezilienciájának stratégiája hosszabb múltra tekint vissza, bár jogilag kötelező erejű szövetségi törvény helyett inkább elnöki direktívák és stratégiák formájában fejlődött. Már 1998-ban kiadtak egy elnöki határozatot (*Presidential Decision Directive,* PDD-63), amely először nevezte meg a kritikus infrastruktúra védelmét nemzetbiztonsági prioritásként.[18]

Ezt követően, a 2001. szeptember 11-i terrortámadások hatására és a Belbiztonsági Minisztérium (Department of Homeland Security, DHS) létrehozásával, az USA fokozta erőfeszítéseit a kritikus infrastruktúrák azonosítása és védelme terén. Az amerikai megközelítés sajátossága, hogy a kritikus infrastruktúrák jelentős része magántulajdonban van, ezért a kormányzat a köz- és magánszféra partnerségére épít a védelem és a reziliencia terén.[19]

A 2013-ban kiadott 21. számú Elnöki Politikai Irányelv (*Presidential Policy Directive,* PPD-21) már a kritikus infrastruktúra biztonsága és rezilienciája címet viselte, jelezve, hogy a fizikai védelem mellett hangsúlyt kapott a gyors helyreállítás képessége is.

A PPD-21 deklarálta, hogy az amerikai kritikus infrastruktúráknak „biztonságosnak és képeseknek kell lenniük ellenállni, valamint gyorsan kiheverni minden lehetséges veszélyt", összhangban a nemzeti felkészültségi rendszerrel a megelőzés, a védelem, a mitigáció, a reagálás és a helyreállítás teljes spektrumában. Az irányelv átfogó politikai célként tűzte ki a sebezhetőségek csökkentését, a lehetséges következmények minimalizálását, a fenyegetések felderítését és megzavarását, valamint a reagálási és helyreállítási képességek javítását a kritikus infrastruktúra területén. Emellett hangsúlyozta a nemzeti egységes fellépés szükségességét, amelynek értelmében a felelősség megoszlik a szövetségi, állami, törzsi és helyi kormányzatok, valamint a magánszektorbeli üzemeltetők között. A szövetségi kormányzat feladata a koordináció javítása különösen a Belbiztonsági Minisztérium, DHS révén, az információmegosztás elősegítése a kormányzati szervek és a magánszektor között, valamint az ágazatspecifikus ügynökségek (Sector-Specific Agencies, ma Sector Risk Management Agencies, SRMA) szerepének erősítése. Az USA 16 kritikus infrastrukturális szektort határozott meg (például energia, víz, élelmiszer és mezőgazdaság, egészségügy, vészhelyzeti szolgáltatások, közlekedés, pénzügyi szolgáltatások, kommunikáció,

[18] Lazari 2022.
[19] The White House 2013.

vegyipar), és mindegyikhez kijelölt egy felelős szövetségi szervet, amely az adott szektor kockázatkezelését és védelmi együttműködését irányítja.

Az USA-ban sokáig iránymutató, önkéntes jellegű keretrendszer működött. A kritikusinfrastruktúra-üzemeltetők jelentős részére nem vonatkozott egységes szövetségi törvény vagy kötelező sztenderd a reziliencia terén, néhány erősen szabályozott ágazat, például nukleáris létesítmények vagy a villamosenergia-hálózat kivételével. Ehelyett a kormányzat ösztönzőkkel, partnerségi programokkal, mint információcsere-fórumokkal, közös gyakorlatokkal, védelmi tervezési útmutatók kiadásával támogatta a magáncégeket abban, hogy javítsák saját biztonsági és üzletmenet-folytonossági terveiket. Ez a megközelítés rugalmasságot biztosított, de sok szakértő rámutatott a korlátaira is, különösen a kibertámadások és az új típusú fenyegetések korában. Az utóbbi években részben a kiéleződő geopolitikai versengés és az infrastruktúrákat érő kibertámadások hatására az USA stratégiája is változóban van.

2024 áprilisában az amerikai elnök új nemzetbiztonsági memorandumot adott ki (*National Security Memorandum,* NSM-22), amely felülírta a korábbi PPD-21 irányelvet, és átfogó erőfeszítést indított a kritikus infrastruktúrák minden fenyegetéssel és veszéllyel szembeni védelmére. Az új stratégia megerősíti a DHS vezető szerepét a kritikus infrastruktúra rezilienciakoordinációjában a Kiber- és Infrastruktúra-biztonsági Ügynökséget (Cyber and Infrastructure Security Agency, CISA) jelölve ki nemzeti koordinátornak, valamint előírja egy kétévente megújítandó *Nemzeti Kockázatkezelési Terv (National Risk Management Plan)* elkészítését, amely áttekinti a legfőbb fenyegetéseket és a kezelésükre tett intézkedéseket. Mindezek mellett a DHS alárendeltségében működik a Nemzeti Kiberbiztonsági és Kommunikáció Integrációs Központ (National Cybersecurity and Communications Integration Center, NCCIC), amely napi 24 órában, heti 7 napon biztosítja szövetségi szinten az eseménykezelési és irányítási feladatokat. Emellett ez a szervezet kapcsolatot biztosít a szövetségi kormány, a hírszerző közösség és a bűnüldözési hatóságok kiber- és kommunikációs szervezetei között.[20] Az NSM-22 megerősíti a 16 kritikus szektor rendszerét és az azokért felelős szövetségi ügynökségek mandátumát, ugyanakkor kiemeli a minimális biztonsági és rezilienciakövetelmények fontosságát az egyes szektorokban, felismerve, hogy pusztán az önkéntes kockázatkezelés nem elegendő a jelenlegi fenyegetettségi környezetben. Ez a retorika egy szigorúbb, szabályozottabb megközelítés felé mozdulást jelez, különösen a kibervédelmi előírások terén, mint például a kötelező incidensbejelentés vagy alapvető kiberhigiéniai követelmények előírányzása bizonyos infrastruktúráknál. Az új stratégia az „előre építkező reziliencia" elvét hangsúlyozza.

Ennek megfelelően a jelentős szövetségi infrastrukturális beruházások (például az infrastruktúra-fejlesztési törvénycsomag keretében) során eleve olyan projekteket finanszíroznak, amelyek figyelembe veszik a jövőbeli éghajlati és biztonsági kockázatokat, így már tervezéskor beépül a reziliencia a rendszerekbe. Az NSM-22 továbbá elismeri, hogy „a reziliencia a hazai védelem és biztonság sarokköve", mivel ellenálló kritikus infrastruktúra nélkül az ország ellenfelei válság vagy konfliktus idején könnyebben okozhatnak zavart a lakosság bizalmában és az ország haderejének mozgósíthatóságában.

[20] Kovács 2018b: 350.

Az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási megközelítései közötti főbb különbségeket és hasonlóságokat az 1. táblázat foglalja össze.

1. táblázat: Az EU és az USA rezilienciaszabályozásának összehasonlítása

Szempont	**Európai Unió**	**Egyesült Államok**
Szabályozás jellege	Jogilag kötelező irányelvek	Elnöki irányelvek, stratégiák
Kormányzási modell	*Top-down,* harmonizált	Decentralizált, partneri
Kritikus szervezetek tulajdonosi szerkezete	Vegyes, jelentős állami szerep	Túlnyomórészt magántulajdon
Reziliencia fókusza	Strukturális és intézményi	Funkcionális és operatív
Magánszektor szerepe	Szabályozott, korlátozottabb	Meghatározó
Kötelező követelmények	Egységes minimumkövetelmények minden tagállamban	Ágazatonként eltérő, növekvő tendencia
Rugalmasság	Korlátozottabb	Magas
Innováció ösztönzése	Közvetett	Erőteljes
Jövőbeni trendek	Minimumkövetelmények erősítése	Szabályozás szigorodása

Forrás: a szerzők szerkesztése

Összefoglalva, az amerikai keretrendszer napjainkra közelít az európaihoz abban az értelemben, hogy egyre inkább felismeri a kötelező minimumkövetelmények szükségességét a reziliencia területén (különösen a kibertérben), miközben továbbra is támaszkodik a magánszektor együttműködési hajlandóságára és innovációjára. Mindkét rendszer hangsúlyozza *az all-hazards* megközelítést, vagyis hogy a kritikus infrastruktúrákat és a kritikus szervezeteket egyaránt védeni kell a természeti katasztrófáktól, káreseményektől és a rosszindulatú támadásoktól.

A koordináció és információmegosztás fontossága szintén közös elem. Az EU a tagállami hatóságok és a Bizottság közötti együttműködést formálissá téve (CER irányelv és munkacsoport révén), míg az USA a szövetségi, állami és magánszereplők közötti partnerséget erősítve igyekszik „nemzeti egységben" kezelni a kihívásokat.[21]

Ugyanakkor a megközelítések különböznek a szabályozási kultúra miatt, mivel Európában jogszabály rögzíti, míg Amerikában ezt sokszor inkább ajánlások és iparági standardok határozzák meg – legalábbis mostanáig. A trend mindkét oldalon a reziliencia intézményesülése és integrálása a mindennapi működésbe, nem csupán válsághelyzeti kérdésként kezelve azt.

Következtetés

A kritikus szervezetek rezilienciája mára a katasztrófavédelem és a nemzetbiztonság kiemelt területévé vált, hiszen a társadalom és a gazdaság ellenálló képessége jelentős részben attól függ, hogy e szervezetek miként képesek megbirkózni a váratlan eseményekkel. A szerzők rámutattak arra, hogy a reziliencia nem statikus állapot, hanem

[21] The White House 2013.

állandóan fejlesztendő folyamat, amely magában foglalja a felkészülést a krízisekre, a hatékony reagálást a bekövetkező rendkívüli eseményekre, valamint a tanulást és alkalmazkodást a válságot követően.

A közigazgatásban és a gazdasági szereplők működésében a reziliencia erősítése olyan reformokat és szervezeti kultúraváltást igényel, amelyek a merev bürokratikus működés helyett a proaktív, rugalmas és együttműködésen alapuló megoldásokat helyezik előtérbe. A lakossági ellátásbiztonság szempontjából pedig kulcsfontosságú, hogy a kritikus szervezetek és infrastruktúrák már békeidőben felkészüljenek a lehetséges rendkívüli eseményekre, ami nemcsak technikai kérdés, hanem stratégiai tervezési és kormányzási feladat is.

A tanulmány célja az volt, hogy összehasonlító elemzés keretében bemutassa az Európai Unió és az Amerikai Egyesült Államok rezilienciaszabályozási megközelítéseit a kritikus szervezetek vonatkozásában, valamint feltárja azokat az intézményi és jogi különbségeket, amelyek meghatározzák az ellenálló képesség fejlesztésének módját.

Az Európai Unió és az Egyesült Államok rezilienciakereteinek összehasonlítása rávilágított arra, hogy bár földrajzilag és intézményileg eltérő környezeti viszonyokról van szó, a célkitűzések hasonlók. Ezek elsődlegesen a szolgáltatások folytonosságának biztosítása minden körülmények között, a társadalom biztonságérzetének fenntartása, valamint a károk minimalizálása és a gyors helyreállítás krízisek idején. Az EU az egységes szabályozás és a tagállami végrehajtás kombinációjával igyekszik koordinált rezilienciát teremteni, míg az USA a decentralizált, partneri megközelítést ötvözi újabban erősödő központi iránymutatással.

Mindkét megközelítésből tanulhatnak egymástól a felek. Az EU-nak hasznos lehet az amerikai rugalmasság és innováció ösztönzése, míg az USA számára az európaiak tapasztalata a minimumkövetelmények és nemzeti stratégiák terén szolgálhat iránymutatásul. A két megközelítés közeledése arra utal, hogy a jövőben egy hibrid modell válhat meghatározóvá, amely ötvözi a jogi kötelezettségek és a partnerségen alapuló megoldások előnyeit. Végső soron a kritikus szervezetek rezilienciájának növelése közös társadalmi érdek, amely megköveteli a tudományos ismeretek, a szakpolitikai döntéshozatal és a gyakorlati végrehajtás szoros összefonódását. A reziliens infrastruktúrák kiépítése a jövő kihívásaival szembeni legjobb befektetés, hiszen erősíti a lakosság biztonságát, a társadalom és a gazdaság stabilitását, ezáltal a nemzetek ellenálló képességét a 21. század sokrétű veszélyeivel szemben.

Felhasznált irodalom

Ambrusz József – Vásárhelyi Örs (2025): A kritikus szervezeti reziliencia és a lakosságfelkészítés nemzetbiztonsági jelentősége a modern fenyegetésekkel szemben. *Nemzetbiztonsági Szemle,* 13(2), 74–93. Online: https://doi.org/10.32561/nsz.2025.2.6

European Commission (2026): *Critical Infrastructure Resilience at EU-level.* Online: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

Gunderson, Lance (2010): Ecological and Human Community Resilience in Response to Natural Disasters. *Ecology and Society,* 15(2). Online: https://doi.org/10.5751/ES-03381-150218
Kádár Pál – Keszely László (2024): A nemzeti ellenálló képesség – a Vbö. V. fejezete. In Kádár Pál (szerk.): *A védelmi és biztonsági szabályozás magyarországi reformja.* Budapest: Ludovika, 185–206. Online: https://doi.org/10.36250/01232_07
Kovács László (2018a): *A kibertér védelme.* Budapest: Dialóg Campus. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf
Kovács László (2018b): *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus.
Mógor Judit – Baloghné Pruha Mária (2025): A kockázat alapú gondolkodás gyakorlati elemei a kritikus szervezeteknél I. rész. *Védelem Tudomány*, 10(3), 14–25. Online: https://doi.org/10.61790/vt.2025.20648
Lazari, Alessandro (2023): Comparing Policy Frameworks: Critical Infrastructure Security and Resilience in the United States and the European Union. In Evans, Carol V. et al. (szerk.): *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency.* Carlisle PA: USAWC Press, 155–170. Online: https://press.armywarcollege.edu/monographs/955
Pálné Kovács Ilona (2023): Az önkormányzati válságkezelés és/vagy reziliencia: Szakirodalmi szemle. *Tér és Társadalom,* 37(1), 3–22. Online: https://doi.org/10.17649/TET.37.1.3465
Profiroiu, Alina Georgiana – Nastacă, Corina-Cristiana (2021): What Strengthens Resilience in Public Administration Institutions? *Eastern Journal of European Studies,* 12(Special Issue), 100–125. Online: https://doi.org/10.47743/ejes-2021-SI05
Székely Iván (2015): Reziliencia: a rendszerelmélettől a társadalomtudományokig. *Replika,* (94), 7–23. Online: http://real.mtak.hu/id/eprint/110083
The White House (2013): *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience.* Washington, DC: Office of the Press Secretary. Online: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/
The White House (2024): *Fact Sheet: Biden-Harris Administration Announces New National Security Memorandum on Critical Infrastructure.* Washington, DC: Office of the Press Secretary. Online: www.presidency.ucsb.edu/documents/fact-sheet-biden-harris-administration-announces-new-national-security-memorandum-critical
Tierney, Kathleen (2015): Disaster Resilience and the Neoliberal Project: Discourses, Critiques, Practices – And Katrina. *American Behavioral Scientist,* 59(10), 15–36. Online: https://doi.org/10.1177/0002764215591187

Jogi forrás

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 1. szám 137–150.
DOI: 10.32567/hm.2026.1.9

Sibalin Iván,[1] Kátai-Urbán Maxim,[2] Cimer Zsolt[3]

Az energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggéseinek értékelése, 2. rész

Assessment of Certain Interrelations between Industrial Safety in the Energy Sector and Environmental Sustainability, Part 2

Absztrakt

A veszélyes anyagokkal foglalkozó üzemek biztonságos működését célzó iparbiztonsági szempontok hatékony érvényesülése a fenntartható fejlődési stratégia sikerének alapvető feltétele. Jelen kutatás fő célja az energiaipari-biztonság és a környezeti dimenzió közötti összefüggések feltárása. A cikksorozat második része a két terület kapcsolódási pontjait a katasztrófavédelem hármas feladatrendszerét alapul véve gyakorlati perspektívából értékeli, a közelmúltban bekövetkezett, jelentős szennyezéssel járó energiaipari balesetek és üzemzavarok során kibocsátott káros anyagok mértékének, a helyreállítás eredményességének, valamint az energetikai rendszerek környezeti kitettségének főként külföldi példáin keresztül.

Kulcsszavak: iparbiztonság, energiaágazat, környezeti fenntarthatóság, baleset, veszélyhelyzeti kibocsátás

[1] Óraadó, Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet, e-mail: sibalin4@gmail.com
[2] Osztályvezető, Semmelweis Egyetem Biztonságtechnikai Igazgatóság Biztonságszervezési Osztály, e-mail: katai.urban.maxim@semmelweis.hu
[3] Dékán, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

Abstract

Ensuring the safe operation of hazardous facilities through the effective implementation of industrial safety measures is a fundamental prerequisite for achieving sustainable development. The primary objective of the present study is to explore the interrelations between the industrial safety in the energy sector and the environmental dimension. The second part of this article series evaluates the points of connection between the two fields from a practical perspective, based on the threefold task system of disaster management. The analysis is conducted through examples of recent energy sector accidents and malfunctions that involved significant environmental contamination, focusing on the quantity of harmful substances released, the effectiveness of recovery efforts, and the environmental vulnerability of energy systems.

Keywords: industrial safety, energy sector, environmental sustainability, accident, emergency release

Bevezetés

A fenntartható fejlődés olyan átfogó stratégiai jövőképet feltételez, amelynek megvalósításához multidiszciplináris megközelítés szükséges. A cikksorozat első része értékelte az iparbiztonság e folyamatban betöltött jelentőségét, valamint megvizsgálta, hogy az annak részszakterületét képező energiaipari-biztonság milyen helyet foglal el a környezeti fenntarthatóságról szóló stratégiai gondolkodásban. A kutatás eredménye értelmében – elméleti és gyakorlati érvekkel alátámasztva – megállapítható, hogy az iparbiztonság a fenntarthatóság környezeti dimenziójában stratégiai jelentőségű szakterületnek minősül. Ugyanakkor az energiaipari-biztonság kérdése korlátozottan jelenik meg a releváns fenntarthatósági diskurzusban, annak ellenére, hogy az energiaágazat katasztrófái rendszerszintű, azaz stratégiai keretek között értelmezhető – egyebek mellett környezeti – hatásokat képesek generálni.

Az alábbi áttekintés az energiaipari-biztonság környezeti fenntarthatóságban betöltött szerepét az iparbiztonság stratégiai jelentőségét megalapozó gyakorlati érvek mentén értékeli. Ez utóbbiak a szakterületnek a környezeti problémák kialakulásának megelőzését, az ipari rendszerek és rendszerelemek meglévő környezeti viszontagságokkal szembeni védelmét, valamint a már bekövetkezett veszélyhelyzeti szennyezések felszámolását célzó rendeltetését tükrözik. Az értékelés alapját a közelmúltban megvalósult, kiterjedt szennyezéssel járó energiaipari balesetek és üzemzavarok során kibocsátott káros anyagok mértékének, a helyreállítás eredményességének, valamint az energetikai rendszerek környezeti kitettségének példái képezik.

Környezeti problémák megelőzése – a veszélyhelyzeti gázkibocsátás kockázata

Köztudomású tény, hogy a fenntartható fejlődés egyik sarokköve az energiatermelés és -fogyasztás minél környezetkímélőbb mennyiségének, minőségének és módjának biztosítása. Ennek részeként főként a – viszonylag könnyen számszerűsíthető – normálüzemi üvegházhatású gázkibocsátás csökkentésére helyeződik a hangsúly. Azonban az energetikai rendszerek veszélyhelyzeti kibocsátása során a káros anyagok mellett szintén jelentős mennyiségű üvegházhatású gáz kerül a környezetbe. A robbanásokkal, tűzesetekkel járó gázkibocsátások, valamint kútfejek, csőszerelvények és csővezetékek szivárgásai vagy tartályhajók olajszivárgása során például jelentős mértékű szénhidrogén távozik a légkörbe.[4] A kockázat jól szemléltethető a kaliforniai Aliso Canyon földgáztároló létesítmény 2015-ben előállt gázszivárgásával, amely során összesen mintegy 80 000 háztartás éves felhasználását meghaladó mennyiségű földgáz szivárgott el,[5] és a katasztrófa közel 600 000 autó éves kibocsátásával egyenlő mértékű hőcsapdahatást generált.[6] Jelzésértékű, hogy egy, a haváriát követően készült elemzés körülbelül 2700 Aliso-típusú létesítményt számolt az Egyesült Államokban.[7] Nem sokkal később, 2018 februárjában egy Ohio állambeli földgázkútnál történt robbanás eredményeként mindössze 20 nap alatt hozzávetőleg 60 kt metán szabadult fel. Ez a mennyiség olyan jelentős európai országok éves metánkibocsátását is meghaladja, mint Franciaország, Spanyolország vagy Norvégia.[8] 2019-ben Louisiana államban a kőolaj- és gázipari üzemeltetői oldalon mintegy 770 millió m^3 elpazarolt földgáz 81%-a kisebb szivárgások miatt veszett kárba.[9] 2020-ban az indiai Asszámban fekvő Baghjan olajmezőn robbanással és hat hónapig tartó tűzesettel is járó gáz- és olajszivárgás komoly károkat idézett elő a régió élővilágában.[10] 2023 júniusában pedig a kazahsztáni Karaturun mezőben vette kezdetét egy 205 napon át tartó olajkútszivárgás, amely során nagyjából 130 kt metán került a környezetbe.[11]

Az elmúlt években, évtizedekben Magyarországon is voltak jelentősebb szénhidrogénipari balesetek. 1985-ben Füzesgyarmaton a Szeghalom 107-es számú fúrási helyen a kitörésgátló leszerelése és megemelése következtében a kútból éghető gáz- és kőolajtermék, valamint paraffin lövellt ki. 1998-ban a nagylengyeli kőolajmező karbantartás során meghibásodott 282/A jelzésű kútjából kiáramló – kén-hidrogén-tartalmú – szén-dioxid terjedése miatt szükségessé vált a környék lezárása, és az alacsonyabb területeken fekvő veszélyeztetett községek lakóinak kitelepítése. 2000-ben a Pusztaszőlős Psz–34. számú kút tört ki a homokszűrő szerelvény cseréje közben. A távozó gáz rövid idő alatt belobbant, a kitörést pedig csak majd három hónappal később sikerült elfojtani.[12] 2010-ben Csepelen tartálytisztítási, anyagma-

[4] IUC UNEP 2000.
[5] Michanowicz 2018.
[6] Warrick 2016.
[7] Michanowicz 2018.
[8] Kann–Almasy 2019.
[9] Synapse Energy Economics – Environmental Defense Fund – Taxpayers for Common Sense [é. n.].
[10] Gogoi–Chetia–Baruah 2022.
[11] Guanter et al. 2024.
[12] Tóth – Siposné Kecskeméthy – Endrődi 2020.

radék-eltávolítási művelet alatt történt tartályrobbanás, a tüzet azonban viszonylag gyorsan sikerült eloltani. 2012-ben és 2018-ban a Zalai Finomító területén bitumentároló tartályok gyulladtak ki: az első tűzeset alapvetően technológiai mulasztásra volt visszavezethető, a második incidens oka pedig tartálytúltöltés volt.[13]

Eltekintve az olyan ritkán előforduló, de extrém pusztító hatású eseményektől, mint az atomerőmű-katasztrófák, a – lényegesebb gyakoribb – szénhidrogénipari baleseteket felsorolt példái is jól mutatják, hogy az energetikai rendszerek veszélyhelyzeti működése globális és lokális szinten egyaránt jelentős környezetterheléssel jár, ezért azok megelőzése, illetve kockázatuk csökkentése a fenntarthatóság szempontjából is kulcsfontosságú.

Az éghajlatváltozással összefüggésben kialakult időjárási viszonyok kockázatai

Az éghajlatváltozást kísérő szélsőséges időjárási viszonyok üzembiztonsági és ellátásbiztonsági szempontból is veszélyeztethetik az energiaipari létesítmények működését. Korunk tipikus környezeti problémái közé tartoznak a növekvő globális átlaghőmérséklet viszontagságai, valamint a villámárvizek romboló hatása.

A magas hőmérséklet kapcsán általánosságban megállapítható, hogy arra a villamos alállomások egyes berendezései meglehetősen érzékenyek,[14] az energiaellátó hálózat túlmelegedhet,[15] és hosszan tartó kánikula esetén a kiszáradt talajban lévő villanypóznák is veszítenek stabilitásukból.[16] Ezen túlmenően a végső hőnyelő (levegő és természetes vizek) hőmérsékletének növekedése csökkentheti az erőművek, a tartós hőséget kísérő gyenge szélmozgás a szélerőművek, a túlhevülés pedig a naperőművek teljesítőképességét,[17] mindeközben az aszály a bioenergia rendelkezésére állását is veszélyeztetheti.[18]

A közelmúltból azonban több konkrét példa is felhozható olyan esetekre, amikor lényegében a globális felmelegedés következményeként került sor incidensre vagy katasztrófaközeli helyzetre az energiaágazatban. 2020-ban az orosz sarkvidék Norilsk városa közelében lévő hőerőmű üzemanyagtartályának sérülése következtében mintegy 21 000 m^3 (17 500 t) dízelolaj okozott jelentős szennyezést az Ambarnaja és Daldykan folyókban, illetve azok környezetében. Az üzemeltető cég tájékoztatása szerint a katasztrófa az olvadó permafrosztra volt visszavezethető.[19] Ugyancsak a felmelegedéssel mutatnak összefüggést a hasonló energetikai baleseteket előidézni képes erdő- és vegetációtüzek. 2016 májusában a kanadai Fort McMurray település környékén alakult ki erdőtűz, amely az erős szél hatására néhány nap alatt már körülbelül 590 000 ha-ra terjedt ki. A rendkívüli pusztítással járó tűzesemény egyebek mellett

[13] Tóth – Siposné Kecskeméthy – Endrődi 2021.
[14] Prudhvi Guddanti et al. 2016.
[15] Jessen 2025.
[16] George 2024.
[17] Aszódi 2018.
[18] Hoover et al. 2020.
[19] Rajendran et al. 2021.

veszélybe sodorta a térség több villamosenergia-vezetékét és átviteli alállomását is,[20] továbbá olajtermelő létesítményeinek működését akadályozta.[21] 14 napon keresztül átlagosan napi 1,2 millió hordó olaj veszett el, számottevő gazdasági hátrányt okozva Alberta tartományban.[22] Bő két évvel később Görögországban, a 102 emberéletet követelő mati erdőtűz-katasztrófa során keletkeztek súlyos károk – a telekommunikációs és a vízellátó rendszerek mellett – az elektromos hálózatban is.[23] Olyan esetre is található példa, amikor a vegetációtüzek egy már nem működő rendszerhez közel kerülve okoztak katasztrófaközeli helyzetet: 2020 áprilisának elején az ukrajnai Csernobiltól nem messze fekvő erdőség gyulladt ki.[24] A néhai atomerőművet megközelítő tűz oltását a száraz idő nehezítette,[25] a lángok azonban nem érintették sem a szarkofágot, sem az atomerőmű betonszarkofágja fölé húzott acélszerkezetet.[26] A csernobili zónában égő tüzet végül 10 nap alatt sikerült eloltani.[27] Nemzetközi sajtónyilvánosságot kapott a Törökország földközi- és égei-tengeri partjainál 2021 nyarán bekövetkezett incidens is, amely során a hőség, a szárazság és az erős szél miatt hevesen terjedő bozóttüzek egy széntüzelésű hőerőmű közvetlen közelébe jutottak. A kialakult helyzet miatt szükségessé vált a robbanásveszélyes vegyi anyagok eltávolítása az erőműből, de a több ezer tonna szénkészlet a térség kiürítését is indokolttá tette. A létesítmény felé terjedő lángokat augusztus elejére sikerült megfékezni.[28] Az energiamix zöldítésével párhuzamosan a megújuló energiát termelő rendszerek és berendezések is egyre inkább ki vannak téve az erdőtűzkockázatnak. 2020 szeptemberében a rendkívül pusztító kaliforniai Creek erdőtűz miatt evakuálni kellett az 1000 MW-os Big Creek vízerőműprojekt alkalmazottjait is. Az extrém magas hőmérséklet hatására megnövekedett légkondicionáló-használat egyébként is jelentősen leterhelte a villamosenergia-rendszert, és közbiztonsági intézkedésként áramszünetet kellett elrendelni azokon a területeken, ahol a száraz időjárás és az erős szél miatt nagy volt a tűzveszély.[29] A 2020-as nyári erdőtüzek által előidézett légszennyezések következtében a Kaliforniai Független Rendszerirányító (CAISO) hálózatának területén a napenergia termelése az eggyel korábbi év ugyanazon két hetével összevetve 13,4%-kal volt alacsonyabb, annak ellenére, hogy az államban 659 MW közmű nagyságrendű kapacitásbővülés valósult meg. Az erdőtüzek füstjét alkotó finom szálló porrészecskék (PM2,5) ugyanis korlátozzák a napelem paneleket érő napsugárzást, így a tüzek súlyossága már az áramellátás fenntartását érintően is aggályokat vet fel.[30]

A hőhullámok, aszályok és erdőtüzek mellett a villámárvizek szintén olyan környezeti problémaként értékelhetők, amelyeknek gyakorisága és intenzitása az éghajlatváltozás következményeként várhatóan megnő,[31] és amelyek az energetikai rendszerelemek

[20] Mondrow 2020.
[21] Besset–Comte 2016.
[22] The University of British Columbia [é. n.].
[23] Efthimiou–Psomiadis–Panagos 2020.
[24] OAH 2020a.
[25] OAH 2020b.
[26] OAH 2020c.
[27] Reevell 2020.
[28] Euronews–AP 2021.
[29] Healy–Taylor–Penn 2020.
[30] Kiss 2020.
[31] ITM 2018: 174.

épségét is veszélyeztethetik. Az árvíz sodrása, nyomása, valamint az általa kiváltott esetleges geodinamikai folyamatok ugyanis károsíthatják az infrastruktúra-elemeket és -hálózatokat, és a víz a korrodálódás kockázatát is fokozza. Ennélfogva indokolt áttekinteni a hirtelen lezúduló nagy mennyiségű csapadékok által előidézett energiaipari haváriaesemények egyes közelmúltbeli példáit is.

2013-ban Colorado államban egy szeptemberi esőzéssorozat utakat, hidakat és egyéb kritikus infrastruktúrát – köztük energetikai rendszerelemeket – megrongáló özönvízszerű áradásokat idézett elő.[32] A Longmont Power & Communications áramszolgáltató vállalat elektromos infrastruktúrájának szignifikáns része megkárosodott, így mintegy 1300 ügyfél maradt körülbelül négy napig áramellátás nélkül.[33] A szénhidrogénipari rendszerelemek is jelentős mértékben sérültek. Több száz olaj- és gázkutat kellett leállítani, és az árvíz által elsodort, törött vezetékek és tárolótartályok fokozták a szennyezés kockázatát. Milliken városban a megrongált tárolótartályokból hozzávetőleg 20 m^3 nyersolaj került a South Platte folyóba.[34] 2017 augusztusában egy Houston melletti vegyi üzemben nagy mennyiségű lokális csapadékra visszavezethető áramkimaradás miatt került sor két robbanásra. A baleset következtében bőr- és szemirritáló füst szennyezte a környezetet, ezért a lakosságot a gyár 2,5 km-es sugarú körében ki kellett telepíteni.[35] 2018 januárjában a kaliforniai Montecitóban pedig hatalmas földgázvezeték-robbanást eredményeztek a heves esőzések törmelékáradásai, több épület kigyulladását okozva.[36]

A viharokkal nemritkán együtt járó villámcsapásoknak jellemzően kitett rendszerelemek közé tartoznak – fizikai elhelyezkedésük és szerkezeti kialakításuk miatt – az átviteli és elosztóvezetékek alkatrészei,[37] a fotovoltaikus panelek[38] és a szélerőművek. E környezeti jelenség azonban bizonyos esetekben komoly balesetek és kiterjedt üzemzavarok konkrét okaként azonosítható. 2019 augusztusában Angliában és Walesben egy villámcsapás és két nagy áramfejlesztő hirtelen meghibásodása miatt közel egymillió ember maradt áram nélkül.[39] 2024-ben, szintén a nyár utolsó hónapjában, Örményország atomerőművét érte villámkár, ami miatt a létesítmény üzemelése biztonsági okokból ideiglenesen leállt, így Jereván több kerületében és néhány más régióban is szünetelt az áramellátás.[40] Nem sokkal később a vitenámi Cai Lậy alállomást ért közvetlen villámcsapás következtében alakult ki tűzzel járó súlyos baleset, áramkimaradást okozva több ezer környékbeli háztartásban.[41] Magyarországon a szénhidrogénipari tartálytüzek és tartályrobbanások egy részét ugyancsak villámcsapás idézte elő, amelyekre példaként az 1974-es, 1982-es és 1985-ös százhalombattai káresemények hozhatók fel.[42]

[32] FEMA 2023.
[33] Esri 2014.
[34] Colorado Department of Natural Resources, Division of Water Resources, Dam Safety Branch [é. n.].
[35] Hoffmann–Szlávik–Cimer 2019: 112–130.
[36] Herrick 2018.
[37] Günther 2023.
[38] Napelem Rendszer [é. n.].
[39] Westbrook 2019.
[40] Reuters 2024.
[41] Thy An Engineering Company 2024.
[42] Tóth – Siposné Kecskeméthy – Endrődi 2021.

A sokszor súlyos következményekkel járó incidensek tanulságai kellőképpen alátámasztják azt a megállapítást, hogy az energetikai rendszerek az éghajlatváltozással szemben különösen kitett infrastruktúrák, amelyek meghibásodása nemritkán további jelentős környezetterheléssel jár. Így a rendszerelemekre gyakorolt károsító hatások azonosítása, valamint a környezeti viszontagságokhoz való alkalmazkodás[43] az energiaágazat esetében kruciális feladat.

1. táblázat: Korunk tipikus környezeti problémái által okozott energiaipari haváriaesemények helyszíne és időpontja

Környezeti problémák			
Felmelegedés, magas hőmérséklet		Viharok	
Olvadó permafroszt	Erdőtűz	Villámárvizek	Villámcsapások
Norilsk (RUS) – 2020	Fort McMurray (CA) – 2016 Mati (GRE) – 2018 Csernobil (UA) – 2020 Creek (USA) – 2020 Égei partok (TUR) – 2021	Colorado (USA) – 2013 Houston (USA) – 2017 Montecito (USA) – 2018	Százhalombatta (HU) – 1974, 1982, 1985 Anglia, Wales (GBR) – 2019 Jereván (ARM) – 2024 Cai Lậy (VIE) – 2024

Forrás: Sibalin Iván szerkesztése

Energiaipari balesetek környezeti hatásai

A fenti példák megfelelően szemléltetik az energiaipari balesetek által előidézhető környezetterhelések lehetséges volumenét, valamint esetenként azok ellátásbiztonsági kihatásait. A kibocsátott káros anyagokra vonatkozó adatok nagyságrendjét figyelembevéve megállapítható, hogy az ilyen haváriaesemények következményeként felborult környezeti egyensúly helyreállítása a környezeti fenntarthatóság jövőképének lényeges eleme. Az energetikai rendszerek veszélyhelyzeti működése által bekövetkezett szennyezések csökkentésének, illetve minél nagyobb mértékű felszámolásának egyik legközvetlenebb módja a kármentesítés. A 219/2004-es kormányrendelet értelmében a kármentesítés

„olyan helyreállítási intézkedés, amely a felszín alatti víz és földtani közeg károsodásának enyhítésére, az eredeti állapot vagy ahhoz közeli állapot helyreállítására, valamint a felszín alatti víz által nyújtott szolgáltatás helyreállítására vagy azzal egyenértékű szolgáltatás biztosítására irányul, így különösen az a műszaki, gazdasági és igazgatási tevékenység, amely a veszélyeztetett, szennyezett, károsodott felszín alatti víz, illetőleg földtani közeg megismerése, illetőleg a szennyezettség, károsodás és a kockázat mértékének csökkentése, megszüntetése, továbbá monitorozása érdekében szükséges”.[44]

[43] Érces–Vass–Ambrusz 2023.
[44] 219/2004. (VII. 21.) Korm. rendelet a felszín alatti vizek védelméről, 3. § 18.

A 220/2004-es kormányrendelet kiterjeszti a definíciót a felszíni vizekre is.[45]

Az energetikai infrastruktúra üzemzavarainak, baleseteinek leginkább kiszolgáltatott környezeti elemek közé tartoznak a vizek, a talaj, illetve a földtani közeg. Ennek látványos megnyilvánulása a kitörések alkalmával a közeli mezőkre szóródó olajos föld, a területre kifolyó olaj, az elsüllyedt berendezések,[46] vagy éppen a folyóba, tengerbe, illetve egyéb természetes vízbe kerülő szénhidrogén-szennyezés. A széntüzelésű erőművek szintén komoly kockázatot jelentenek a talaj és a vizek épségére.[47] Hazánkban az ország vízrajzi helyzeténél fogva fokozott kockázattal jár a környezetszennyező anyagok élővizekbe jutása: a veszély adott esetben több száz kilométer távolságban is jelentkezhet.[48]

A szénhidrogénipari káreseményeket követő, 50%-hoz közelítő, illetve esetenként azt jelentősen meghaladó arányú károsanyag-eltávolítás (illetve -kezelés) példái között említhető a Tennessee állambeli Kingston fosszilis erőmű 2008-as hamuzagy-katasztrófája, a 2010-es Deepwater Horizon olajkatasztrófa, Brazília északkeleti partjának 2019/2020-as olajszennyezése, valamint a Colonial Pipeline 2020/2021-es benzinszivárgása.

A kingstoni incidens során az erőmű lerakóján történt gátszakadás, amelyen keresztül hamuzagy ömlött ki 4 millió m^3-t meghaladó mennyiségben, beszennyezve a közeli folyókat, lakóépületeket és mezőgazdasági termőterületeket.[49] A helyreállítási munkák első fázisa során megközelítőleg 2,7 millió m^3, majd a második fázis keretében hozzávetőleg 1,7 millió m^3 hamut távolítottak el.[50] Ennek összege mennyiségét tekintve lefedi a kiáramlott anyag mértékét, azonban teljes eltávolításról nem beszélhetünk, hiszen a begyűjtött hamu minden bizonnyal tartalmazott más, a természetes közegben eleve meglévő anyagot, üledéket. Az Amerikai Környezetvédelmi Ügynökség online felületén elérhető becsült adat szerint 380 000 m^3 hamuzagy maradhatott vissza.[51] Következésképpen a teljes kibocsátás nagyjából 90%-át sikerült begyűjteni. A Deepwater Horizon fúrótorony robbanását az Egyesült Államok legnagyobb tengeri olajszennyezéseként tartják számon. Az egykor a Louisiana állam partjainak közelében üzemelő mélytengeri olajfúró platform a szövetségi kormány tisztviselőinek becslése szerint 84 nap alatt több mint 4,9 millió hordó nyersolajat bocsátott az óceánba. Ennek mintegy 17%-át sikerült visszanyerni, 5%-át a helyszínen elégetni, 3%-át lefölözni, 16%-át pedig diszpergálni. Így emberi beavatkozással a szennyezés nagyjából 41%-át lehetett valamilyen módon kezelni. Az olajnak körülbelül 37%-a természetes folyamatok révén diszpergálódott, feloldódott vagy elpárolgott.[52] Nehezen meghatározható eredményesség jellemezte a brazíliai eseményeket, tekintettel arra, hogy csak tág intervallumok – körülbelül 5000 és 12 000 m^3 – között becsülhető meg az óceánba került olaj teljes mennyisége, és ez volt a trópusi óceánokban megfigyelt legnagyobb területi kiterjedésű (2890 km hosszan elterülő) olajszennyezés.

[45] 220/2004. (VII. 21.) Korm. rendelet a felszíni vizek minősége védelmének szabályairól, 3. § 41.
[46] Tóth – Siposné Kecskeméthy – Endrődi 2021.
[47] Jones et al. 2016: 46.
[48] Hoffmann et al. 2015.
[49] Kovacsics 2024: 52–62.
[50] U.S. Environmental Protection Agency 2017a: 3–5.
[51] U.S. Environmental Protection Agency 2017b.
[52] Ramseur 2010.

Mindazonáltal a partokon összegyűjtött mintegy 5380 t olaj csaknem 100%-át eltávolították.[53] Nagyságrendjéről emlékezetes a Colonial Pipeline észak-karolinai katasztrófája is, amely az Egyesült Államok történetének legnagyobb szárazföldi üzemanyag-szivárgásának helyszíne. Becslések szerint a meghibásodott vezetékből hozzávetőleg 47 600 hordó benzin szivárgott ki a szabadba két-három hét leforgása alatt,[54] amelynek mintegy 85%-át sikerült visszanyerni a 2022-es év végéig,[55] 2024-es hírek pedig a remediációs munkálatok folytatásáról számolnak be.[56]

A bemutatott energiaipari balesetek tanulságaként fogalmazható meg, hogy az energetikai rendszerek veszélyhelyzeti működése során keletkezett szennyezések felszámolása körülményes feladat, amelynek hatékonysága számos tényezőtől függ. A katasztrófák súlyosságára és gyakoriságára tekintettel ezért konstatálható, hogy a kármentesítés technológiájának további fejlesztése a környezeti fenntarthatóság megvalósításának szükségszerű eleme.

2. táblázat: A vizsgált balesetek során kibocsátott és kezelt szennyező anyagok volumene

Évszám	Esemény	A kibocsátott szennyező anyag mennyisége	A kezelt szennyező anyag becsült arányszáma
2008	Kingston	> 4 millió m^3 hamuzagy	90%
2010	Deepwater Horizon	> 4,9 millió hordó nyersolaj	41%
2019/20	Északkelet-Brazília	~ 5380 t nyersolaj (partokon)	közel 100%
2020/21	Colonial Pipeline	~ 47 600 hordó benzin	2022 végéig 85%

Forrás: Sibalin Iván szerkesztése

Összegzés

Napjaink technológiai és egyéb globális szintű kihívásai közepette konstans és hosszú távú aggályként vannak jelen bolygónk életében a természeti környezettel kapcsolatos kockázatok, amelyek kezelése egyre sürgetőbb és sokrétű beavatkozást igényel. A fenntartható fejlődés (környezeti dimenzió) tekintetében az iparbiztonság is stratégiai jelentőségű szakterületként értelmezhető, ugyanis annak elhanyagolása, illetve a releváns stratégiai tervezésből való kiiktatása minden bizonnyal meghiúsítaná vagy jelentősen megnehezítené a környezeti fenntarthatóság jövőképének megvalósítását. Az iparbiztonság ebbéli funkciója elméleti és gyakorlati érvekkel is alátámasztható. Az előbbiek közé sorolható a fenntarthatósági és ipari biztonsági szempontok egyidejű megléte a hatályos stratégiai keretrendszerben, az iparbiztonság absztrakt ökológiai válságkezelési szerepe, valamint a szakterület multidiszciplináris jellege. Az utóbbiak közé tartozik az iparbiztonságnak a környezeti problémák megelőzésében, a már meglévő környezeti problémákkal szembeni védekezésben, valamint a környezeti egyensúly helyreállításában betöltött rendeltetése.

[53] Soares et al. 2022.
[54] Duncan 2022.
[55] Chemtob 2023.
[56] Dellinger 2024.

Az iparbiztonság részét képező energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggései a gyakorlati érvek mentén szemléletes módon értékelhetők. A cikkben bemutatott szénhidrogénipari incidensek által okozott légszennyezés volumene intő jel lehet arra nézve, hogy az energetikai rendszerek veszélyhelyzeti működése során is hatalmas mennyiségű üvegházhatású gáz áramlik a légkörbe, ezért az ilyen balesetek és üzemzavarok által előidézhető környezeti problémák megelőzése alapvető fenntarthatósági kritérium.

Az éghajlatváltozást kísérő tipikus környezeti problémák között említhető a globális felmelegedés, valamint a villámárvizek növekvő intenzitása és gyakorisága. Az energiaágazat mindkét jelenség által erősen érintett, üzembiztonsági és ellátásbiztonsági szempontból egyaránt. Számos – jelentős károsanyag-kibocsátással járó – hazai és külföldi eset tanúsítja, hogy a megváltozott meteorológiai feltételek súlyos balesetek forrásai lehetnek, ezért az energetikai rendszereknek és rendszerelemeknek a meglévő környezeti problémáktól való megóvása, vagy másképp szólva az azokhoz való alkalmazkodása ugyancsak lényeges feltétele a környezeti fenntarthatóságnak.

A havériajellegű eseményekből eredő környezetterhelés felszámolásának egyik legközvetlenebb módja a kármentesítés. Az energetikai incidensek következményeinek elhárítása sokszor összetett és körülményes feladat, sikerét számos olyan tényező befolyásolhatja, amelyre a helyreállítási munkát végző szakembereknek nincsen ráhatása. Ezzel együtt a cikkben példaként felhozott, súlyos szennyezéssel járó szénhidrogénipari események vonatkozásában a környezetbe került káros anyag mennyiségének kezelése néhány esetben kifejezett eredményességgel zárult. Ezt szem előtt tartva a kármentesítés technológiájának fejlesztése a környezeti fenntarthatóság szempontjából kiváltképp fontos, különös tekintettel az energiaágazatban előállt balesetek gyakoriságára és azok pusztító, sokszor maradandó környezetkárosodást okozó hatására.

A jelen cikkel kapcsolatos kutatómunka 2025. szeptember 30-án zárult.

Felhasznált irodalom

Aszódi Attila (2018): A nyári hőhullám hatása a villamosenergia-termelésre. *Láncreakció – Aszódi Attila információs blogja.* 2018. augusztus 22. Online: https://aszodiattila.blog.hu/2018/08/22/a_nyari_hohullam_hatasa_a_villamosenergia-termelesre

Besset, Julien – Comte, Michel (2016): Canadian Oil Hub Works to Restore Power, Eyes Resuming Full Oil Output. *AFP,* 2016. május 11. Online: https://sg.news.yahoo.com/canadas-fire-ravaged-fort-mcmurray-works-restore-utilities-171504156.html

Chemtob, Danielle (2023): Millions of Gallons of Gasoline Spilled From a Pipeline in the Charlotte Area, and It's Still Being Cleaned Up. *Axios,* 2023. március 21. Online: www.axios.com/local/charlotte/2023/03/21/millions-of-gallons-of-gasoline-spilled-from-a-pipeline-in-the-charlotte-area-and-its-still-being-cleaned-up-323376

Colorado Department of Natural Resources, Division of Water Resources, Dam Safety Branch [é. n.]: *After Action Report – Colorado Flooding 2013.* Online: https://

damsafety.org/sites/default/files/files/AAR%20DWR%20DSB%20Flooding%202013.pdf
Dellinger, Derek (2024): Work Still Needs to Be Done 4 Years After Historic Huntersville Fuel Spill. *Queen City News,* 2024. augusztus 13. Online: www.qcnews.com/news/colonial-pipeline/work-still-needs-to-be-done-four-years-after-huntersville-fuel-spill/
Duncan, Charles (2022): N.C. Nature Preserve, Site of the Worst Onshore Fuel Spill in the U.S., Still Closed 2 Years Later. *Spectrum News,* 2022. augusztus 4. Online: https://spectrumlocalnews.com/nc/charlotte/environment/2022/08/04/n-c—nature-preserve—site-of-the-worst-onshore-fuel-spill-in-the-u-s—-still-closed-2-years-later
Efthimiou, Nikolaos – Psomiadis, Emmanouil – Panagos, Panos (2020): Fire Severity and Soil Erosion Susceptibility Mapping Using Multi-Temporal Earth Observation Data: The Case of Mati Fatal Wildfire in Eastern Attica, Greece. *Catena,* 187. Online: https://doi.org/10.1016/j.catena.2019.104320
Esri (2014): Managing Recovery Efforts with Mobile GIS after Colorado Floods. *Esri ArcNews,* 2014. ősz. Online: www.esri.com/about/newsroom/arcnews/managing-recovery-efforts-with-mobile-gis-after-colorado-floods
Euronews – AP (2021): Sikerült megfékezni a széntüzelésű hőerőmű felé terjedő erdőtüzet Törökországban. *Euronews,* 2021. augusztus 5. Online: https://hu.euronews.com/2021/08/05/sikerult-megfekezni-a-szentuzelesu-hoeromu-fele-terjedo-erdotuzet-torokorszagban
Érces Gergő – Vass Gyula – Ambrusz József (2023): Épületek károsító hatásokkal szembeni rezilienciájának jellemzői. *Polgári Védelmi Szemle,* 15(különszám), 117–130. Online: https://kvi.uni-nke.hu/document/kvi-uni-nke-hu/%C3%96sszerakott%20PV%20Szemle%20cikkek_02_24_Szerkesztett.pdf#page=117
FEMA (2023): *2013 Colorado Floods. A Decade of Recovery and Building Resilience.* U.S. Department of Homeland Security, 1–21. Online: www.fema.gov/sites/default/files/documents/fema_r8-2013-colorado-floods-decade-recovery-building-resilience.pdf
George, Richard (2024): The Impact of Global Warming on the Durability of Utility Poles. *Factor This,* 2024. április 15. Online: www.renewableenergyworld.com/energy-business/the-impact-of-global-warming-on-the-durability-of-utility-poles/
Gogoi, Swapnali – Baruah, Bubu – Chetia, Annekha (2022): Baghjan Fire: a Case Study of the '2020 Assam Gas and Oil Leak' at Baghjan Oil Field, Tinsukia, Assam. *5th World Congress on Disaster Management: Volume II.* London: Routledge, 483–497. Online: https://doi.org/10.4324/9781003341932-51
Guanter, Luis et al. (2024): Multisatellite Data Depicts a Record-Breaking Methane Leak from a Well Blowout. *Environmental Science & Technology Letters,* 11(8), 825–830. Online: https://pubs.acs.org/doi/10.1021/acs.estlett.4c00399
Günther, Reinhard (2023): Illuminating the Dark Side – Lightning's Assault on Power Grids. *CLOUGLOBAL News,* 2023. július 18. Online: https://clouglobal.com/illuminating-the-dark-side-lightnings-assault-on-power-networks/

Healy, Jack – Taylor, Kate – Penn, Ivan (2020): California Wildfires: Extreme Heat Turns State Into a Furnace. *The New York Times,* 2020. szeptember 7. Online: www.nytimes.com/2020/09/07/us/ca-wildfires-heatwave.html

Herrick, Kelly Mahan (2018): The Year in Review 2018. *Montecito Journal,* 2018. december 27. Online: www.montecitojournal.net/2018/12/27/the-year-in-review-2018/

Hoffmann Imre et al. (2015): Iparbiztonsági kockázatok Magyarországon. *Védelem Online: Tűz- és katasztrófavédelmi szakkönyvtár,* 22(1). Online: www.vedelem.hu/letoltes/anyagok/546-iparbiztonsagi-kockazatok-magyarorszagon.pdf

Hoffmann Imre – Szlávik Lajos – Cimer Zsolt (2019): Árvíz által okozott katasztrófák iparbiztonsági vetületei. *Védelem Tudomány,* 4(különszám), 112–130. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13306/10739

Hoover, Amber et al. (2020): Drought Impacts on Bioenergy Supply System Risk and Biomass Composition. In Ondrasek, Gabrijel (szerk.): *Drought – Detection and Solutions.* Intechopen. Online: https://doi.org/10.5772/intechopen.85295

ITM (2018): A 2018–2030 közötti időszakra vonatkozó, 2050-ig tartó időszakra is kitekintést nyújtó második Nemzeti Éghajlatváltozási Stratégia. 23/2018. (X. 31.) OGY határozat melléklete. Online: https://njt.hu/jogszabaly/2018-23-30-41

IUC UNEP (2000): *Climate Change Information Sheet 22. How Human Activities Produce Greenhouse Gases.* Online: https://unfccc.int/cop3/fccc/climate/fact22.htm

Jessen, Jasmin (2025): How do Heatwaves Affect Power Grids? *Energy Digital,* 2025. június 30. Online: https://energydigital.com/news/climate-change-how-heatwaves-are-affecting-power-grids

Jones, Dave et al. (2016): *Europe's Dark Cloud – How Coal-burning Countries are Making Their Neighbours Sick.* Brussels: CAN Europe – HEAL – WWF European Policy Office – Sandbag. Online: https://wwf.hu/wp-content/uploads/2023/05/1467799428_Dark_cloud_report.pdf

Kann, Drew – Almasy, Steve (2019): A Natural Gas Blowout in Ohio Released More Methane Than Many Countries Do in an Entire Year. *CNN,* 2019. december 18. Online: https://edition.cnn.com/2019/12/17/us/ohio-exxon-mobil-methane-leak-satellite-climate-change

Kiss Ernő (2020): A kaliforniai erdőtüzek lehúzták a napelemek múlt havi termelését. *Magyar Napelem Napkollektor Szövetség,* 2020. október 1. Online: www.mnnsz.hu/a-kaliforniai-erdotuzek-lehuztak-a-napelemek-mult-havi-termeleset/

Kovacsics István (2024): Szénerőművek környezetbarát hamukezelése – az MVM megoldás. *Energiaforrás,* 60(1), 52–62. Online: https://mvm.hu/-/media/MVMHu/Documents/Media/Mediatartalmak/Energiaforras/MVM-Energiaforras_2024_1_web_jav.pdf

Michanowicz, Drew (2018): Op-Ed: The Aliso Canyon Gas Leak Was a Disaster. There Are 10,000 More Storage Wells Out There Just Like It. *Los Angeles Times,* 2018. május 14. Online: www.latimes.com/opinion/op-ed/la-oe-michanowicz-aliso-canyon-gas-leak-20180514-story.html

Mondrow, Ian A. (2020): The Fort McMurray Wildfire Cases: Life After Stores Block. *Gowling WLG,* 2020. szeptember 30. Online: https://gowlingwlg.com/en/insights-resources/articles/2020/the-fort-mcmurray-wildfire-cases

Napelem Rendszer [é. n.]: *Féltsük az időjárástól a napelemeket?* Online: https://napelemrendszer.info/feltsuk-az-idojarastol-a-napelemeket.html

OAH (2020a): Magyarországon nem emelkedett a háttérsugárzás a Csernobil melletti erdőtűz miatt. *OAH Hírek,* 2020. április 6. Online: https://nyomtatvany.oah.hu/web/v3/OAHPortal.nsf/web?OpenAgent&article=news&uid=32A2D6D8A302266FC125854200476102

OAH (2020b): Elhúzódnak az oltási munkálatok Csernobilban. *OAH Hírek,* 2020. április 30. Online: www.haea.hu/web/v3/OAHportal.nsf/web?OpenAgent&article=news&uid=98932EF9014FF799C125855A003DF601

OAH (2020c): Reagálás a közösségi médiában megjelenő álhírekre, félrevezető, aggodalmat keltő információkra. *OAH Hírek,* 2020. április 9. Online: www.haea.gov.hu/web/v3/oahportal.nsf/web?OpenAgent&article=news&uid=96A32D026F10AAB0C1258545006A6FA0

Prudhvi Guddanti, Kishan et al. (2016): A Comprehensive Review: Impacts of Extreme Temperatures due to Climate Change on Power Grid Infrastructure and Operation. *IEEE Access,* 4, 1–40. Online: https://arxiv.org/pdf/2410.08425v2

Rajendran, Sankaran et al. (2021): Monitoring Oil Spill in Norilsk, Russia Using Satellite Data. *Nature Scientific Report,* 11, 3817. Online: https://doi.org/10.1038/s41598-021-83260-7

Ramseur, Jonathan L. (2010): *Deepwater Horizon Oil Spill: The Fate of the Oil.* (Summary). Congressional Research Service. Online: www.congress.gov/crs_external_products/R/PDF/R41531/R41531.10.pdf

Reevell, Patrick (2020): Ukraine Says Wildfires Close to Chernobyl Are Extinguished After Rain Falls. *ABC News,* 2020. április 14. Online: https://abcnews.go.com/International/ukraine-wildfires-close-chernobyl-extinguished-rain-falls/story?id=70138987

Reuters (2024): Armenia's Nuclear Power Plant to Resume Work After Lightning Strike. *Reuters,* 2024. augusztus 31. Online: www.reuters.com/world/europe/armenia-says-lightning-strike-shuts-down-nuclear-power-station-interfax-reports-2024-08-31/

Soares, Marcelo Oliveira et al. (2022): The Most Extensive Oil Spill Registered in Tropical Oceans (Brazil): The Balance Sheet of a Disaster. *Environmental Science and Pollution Research,* 29, 19869–19877. Online: https://doi.org/10.1007/s11356-022-18710-4

Synapse Energy Economics – Environmental Defense Fund – Taxpayers for Common Sense [é. n.]: *Methane Waste and Pollution in Louisiana.* Online: www.edf.org/sites/default/files/2023-09/LA%20methane%20waste%20%20pollution%20analysis%202023-04.pdf

The University of British Columbia [é. n.]: *Fort McMurray and the Fires of Climate Change.* Online: https://cases.open.ubc.ca/fort-mcmurray-and-the-fires-of-climate-change/

Thy An Engineering Company (2024): Lightning Strike Causes Fire at Cai Lay Substation: Risks and Lessons Learned. *TAEC Lightning News,* 2024. szeptember 2. Online: https://thyan.vn/en/lightning-strike-causes-fire-at-cai-lay-substation-risks-and-lessons-learned

Tóth András – Siposné Kecskeméthy Klára – Endrődi István (2020): A magyar szénhidrogéniparban előfordult katasztrófák, azok tanulságai és a megelőzés módozatai 1. rész. *Hadmérnök,* 15(4), 119–140. Online: https://doi.org/10.32567/hm.2020.4.9

Tóth András – Siposné Kecskeméthy Klára – Endrődi István (2021): A magyar szénhidrogéniparban előfordult katasztrófák, azok tanulságai és a megelőzés módozatai 2. rész. *Hadmérnök,* 16(1), 129–144. Online: https://doi.org/10.32567/hm.2021.1.8

U.S. Environmental Protection Agency (2017a): *TVA Kingston Site Case Study – Revitalization of the Wetlands, Embayments and Emory River.* Online: www.epa.gov/sites/default/files/2018-02/documents/tva_kingston_site_case_study_2017.pdf

U.S. Environmental Protection Agency (2017b): *Watts Bar Reservoir Ecosystem Adjacent to TVA Kingston Facility Returns to Baseline Conditions.* Online: https://19january2017snapshot.epa.gov/newsreleases/watts-bar-reservoir-ecosystem-adjacent-tva-kingston-facility-returns-baseline_.html

Warrick, Joby (2016): California Gas Leak Was the Worst Man-Made Greenhouse-Gas Disaster in U.S. Study Says. *The Washington Post,* 2016. február 25. Online: www.washingtonpost.com/news/energy-environment/wp/2016/02/25/california-gas-leak-was-the-worst-man-made-greenhouse-gas-disaster-in-u-s-history-study-says/

Westbrook, Ian (2019): Lightning Strike 'Partly to Blame' for Power Cut. *BBC,* 2019. augusztus 20. Online: www.bbc.com/news/business-49402296

Jogi források

219/2004. (VII. 21.) Korm. rendelet a felszín alatti vizek védelméről. Online: https://njt.hu/jogszabaly/2004-219-20-22

220/2004. (VII. 21.) Korm. rendelet a felszíni vizek minősége védelmének szabályairól. Online: https://njt.hu/jogszabaly/2004-220-20-22

HADMÉRNÖK
FÓRUM
21. évfolyam (2026) 1. szám 151–166.
DOI: 10.32567/hm.2026.1.10

Somogyi Zoltán[1]

A kompenzálatlan hőterhelést előidéző mikroklimatikus viszonyok kialakulásának dinamikája a tűzoltó védőruházatban

Dynamics of the Formation of Microclimatic Conditions Causing Uncompensated Heat Stress in Firefighting Protective Clothing

Absztrakt

Jelen kutatás a tűzoltó védőruházaton belüli mikroklíma változásainak dinamikáját és hatását vizsgálta a maghőmérsékletre. A vizsgálat alapkérdése volt, hogy kialakulhatnak-e hőterhelést előidéző mikroklimatikus tényezők a tűzoltó védőruházatban a beavatkozások kezdeti szakaszában a tényleges tűzoltást megelőzően. Hogyan változik a maghőmérséklet és bőrhőmérséklet, milyen ütemben alakul ki a kompenzálatlan hőterhelés? Van-e lényeges különbség azonos munkavégzés és külső környezeti feltételek mellett védőruházatot viselve és sportruházatban végrehajtott terhelés élettani mutatói között. A bevetési ruhában (BEV) és a sportruházatban végzett (kontroll, KON) 35 perc időtartamú 9±1 MET egységben megszabott terheléses vizsgálaton a csoportok közötti eredmények alapján két csoport maghőmérséklet (Tc) értékei között jelentős eltérés mutatkozott. BEV-csoportban (átlag [M] = 38,36; szórás [SD] = 0,116) és a KON-csoportban (M = 37,99; SD = 0,055) a Tc-értékek szignifikáns (p = 0,010) különbséget mutattak. A teszt végén detektált pulzusszámok (HR) esetében a BEV (M = 163,4; SD = 8,414) és KON (M = 133; SD=9,848) csoportok között a statisztikai elemzés szintén jelentős különbséget mutatott ki (p = 0,0127). Az adatokból látható, hogy azonos külső terhelés mellett a kontrollcsoportban sem a maghőmérséklet,

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: zoltan.somogyi@katved.gov.hu

sem a bőrhőmérséklet, sem a pulzusszám nem éri el a BEV-csoport értékeit. A védőruházaton belüli mikroklímára jellemző volt, hogy a teszt végén az átlagos légréshőmérséklet 33,58 °C, (SD 1,03), és a relatív páratartalom 80,95% (SD 9,89) volt. Az eredmények alapján igazolható a feltételezés, hogy a beavatkozások kezdeti szakaszában olyan mikroklimatikus viszonyok alakulhatnak ki a védőruházatban, amelyek kompenzálatlan hőterhelés kialakulásához vezethetnek. A mérési adatok további matematikai és statisztikai elemzései kimutatták, hogy a BEV-csoport tagjainál a kompenzálatlan hőterhelést jelző markerek jellemzően a 15. és 18. perc között jelentek meg

Kulcsszavak: kompenzálatlan hőstressz, maghőmérséklet, védőruházat, tűzoltó

Abstract

This research examined the dynamics of microclimate changes within firefighter protective clothing and their effect on core body temperature. The basic question of the study was whether microclimatic factors causing heat stress can develop in firefighter protective clothing during the initial phase of interventions, before the actual firefighting. How do core temperature and skin temperature change, and at what rate does uncompensated heat stress build up? Is there a significant difference between the physiological indicators of exertion performed while wearing protective clothing and those performed in sportswear, under the same working conditions and external environmental conditions? In a 35-minute exercise test performed in the protective clothing (BEV) and sportswear (control, KON) at a specified load of 9±1 MET units, the results between the groups showed a significant difference between the core body temperature (Tc) values of the two groups. In the BEV group (mean [M] = 38.36; standard deviation [SD] = 0.116) and the KON group (M = 37.99; SD = 0.055), the Tc values showed a significant (p = 0.010) difference. In the case of the heart rates (HR) detected at the end of the test, statistical analysis also showed a significant difference between the BEV (M = 163.4; SD = 8.414) and KON (M = 133; SD = 9.848) groups (p = 0.0127). The data show that, under the same external load, neither the core temperature, skin temperature, nor heart rate in the control group reached the values of the BEV group. The microclimate inside the protective clothing was characterised by an average air temperature of 33.58 °C (SD 1.03) and the relative humidity was 80.95% (SD 9.89). The results confirm the assumption that in the initial phase of the interventions, microclimatic conditions may develop inside the protective clothing that can lead to uncompensated heat stress. Further mathematical and statistical analysis of the measurement data showed that markers indicating uncompensated heat stress typically appeared between the 15th and 18th minutes in members of the BEV group.

Keywords: uncompensable heat stress, core body temperature, protective clothing, firefighters

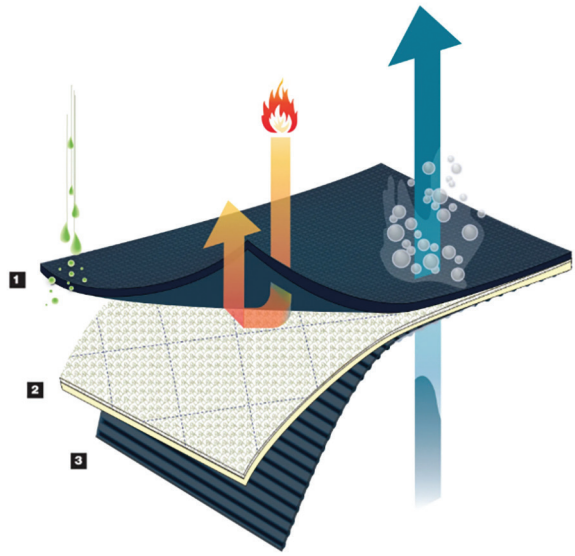
Bevezető

A tűzoltók munkavégzése napjainkban elképzelhetetlen védőruházat nélkül. Érdemes azonban vizsgálat tárgyává tenni, hogy a magas fokú védelmi képességekkel rendelkező védőruházat, amely megóvja viselőjét számos káros külső hatástól, milyen kihívások elé állítja viselője szervezetét. A tűzoltói munkán kívül számos emberi munkatevékenység kedvezőtlen, sőt olykor szélsőséges környezeti feltételek mellett valósul meg. A mélyművelésű bányászattól az űrutazásig terjedő skálán találkozhatunk számos olyan tevékenységgel, ahol az egyén a jelentős fizikai terhelés mellett magas páratartalomnak és/vagy direkt hősugárzásnak lehet kitéve. Az ilyen magas hőmérsékleten végzett munka kedvezőtlen hatást gyakorolhat az emberi teljesítményre és egészségre, fokozott megterhelést, teljesítménycsökkenést és hővel kapcsolatos megbetegedéseket okozhat.[2] A hőterhelés áttételesen a munkavégzés számos más kockázati tényezőjét is negatívan befolyásolhatja, módosítva vagy súlyosbítva a gyakori veszélyek kockázatát. A hőterheléssel kapcsolatos ártalmak sokkal gyakoribbak azon munkaköröknél, ahol személyi védőfelszerelést kell viselni a kémiai, biológiai, fizikai (mechanikai, termikus, sugárzási) vagy egyéb veszélyeknek való kitettség csökkentése érdekében.

A tűzoltó védőruházat felépítése és hatása a szervezetre

A tűzoltó bevetési védőruhákat funkcionális nézőpontú megközelítésben három kategóriában vizsgálhatjuk: biztonság, hatékonyság és komfort. Könnyen belátható, hogy a felsorolás sorrendje egyben fontossági sorrendet is jelez. Elsőként, a ruházat alapvető célja az emberi test és a környezet közötti védőrétegként a káros hatások eliminálása.[3] Ennek érdekében a ruházat többek közt szigetel a víztől és a hőhatásoktól, lángálló, véd a mechanikai sérülések ellen, ellenáll a vegyi anyagok károsító hatásainak és gátolja a statikus feltöltődést. Ezen erősen eltérő jellegű veszélyezetető tényezők elleni védelmet a bevetési védőruha különböző anyagokból álló, többrétegű szerkezete biztosítja (1. ábra). A külső borító réteg főként a láng- és mechanikai védelemért, a középső membránréteg a nedvesség kétirányú áramlásának szabályzásáért és hőszigetelésért felel. A legbelső réteg a testbélés, amely a lélegző membránt és hordozórétegét védi a viselés közbeni sérülésektől és az izzadság elvezetését végzi.[4]

[2] Vitrai 2021.
[3] Horváth 2018.
[4] Kutasi 2025.



1. ábra: A tűzoltó védőruházat rétegei (1. külső réteg, 2. membrán, 3. testbélés)
Forrás: https://sioenfire.com/en/expertise/assemblies

A másodlagos funkcionális szempont a hatékonyság, mivel lényeges, hogy az öltözék a munkavégzés hatékonyságát a lehető legkisebb mértékben csökkentse.[5] A feladat-végrehajtás szempontjából a hatékonyságot befolyásoló tényező lehet a ruházat súlya, az egyes rétegek anyagainak hajlékonysága, rugalmassága, az ízületi mozgástartományokra gyakorolt hatása. A harmadlagos tényező, a viselés komfortja, már erősen szubjektív fogalom. A védőruha műszaki megfelelősége és az általa nyújtott védelem maximális szintje sok esetben ellentétes viselőjének kényelmi igényeivel. Bár a gyártók és a tervezők fejlesztéseik során igyekeznek ezen igényeket is maximálisan figyelembe venni, a gyakorlati alkalmazás során nyert tapasztalat az, hogy tartós viselésük az elhúzódó beavatkozások alkalmával gyakran feszegeti az elviselhető fiziológiai terhelés objektív és szubjektív határát. A védőruházat a munkakörnyezetet, a tűzoltókat körülvevő fizikai teret külső és belső részre osztja. A külső tér, a tűzoltókat a kárhelyszínen körülvevő fizikai tér, amelyet az adott hely időjárási viszonyait mutató meteorológiai mérőszámai (a hőmérséklet, a páratartalom, a légmozgás), valamint a tűzeset környezeti tényezőket módosító hatásai (a tűz következtében keletkező hősugárzás és módosult hőmérséklet, valamint az oltóvíz párolgásából keletkező páratartalom) írnak le. Ezt nevezhetjük makrokörnyezetnek. A belső környezet a védőruházat és a test közötti légrésben kialakuló mikrokörnyezet. A mikrokörnyezet klímájának kialakulására a metabolikus hőtermelés hatására keletkező hő és az izzadságból keletkező pára, valamint a természeti környezet és a tűzeset által kialakított makrokörnyezet van hatással.

[5] Pántya 2018.

A mikrokörnyezetet befolyásoló tényezők

Érdemes elsőként elméleti oldalról megvilágítani, hogyan alakul ki a védőruházaton belüli mikrokörnyezet klímája. Az emberi szervezet az állandóság, a homeosztázis fenntartása érdekében hőtermelő és hőleadó folyamatok segítségével bizonyos határok között szabályozni képes belső hőmérsékletét a külső hőhatások okozta eltérések kompenzálása érdekében.[6] Meleg környezetben, fizikai aktivitás közben a hőszabályzás feladata a felesleges hő leadása. A hőcsere nagy része a bőr felületén történik, főként konvekció, sugárzás és párolgás útján. A környezeti hőmérséklet emelkedésével a konvekciós és radiációs hőátadás csökken, ami azt jelenti, hogy az emberi test egyre inkább az izzadság elpárologtatására támaszkodik a felesleges hő elvezetéséhez. Ha a külső körülmények, a léghőmérséklet, a hősugárzás, páratartalom, a légsebesség és a ruházat kombinációja elegendő hőelvezetést tesz lehetővé a belső hőtermelés mértékének ellensúlyozásához, a test maghőmérsékletének emelkedése mérsékelt marad, azaz kompenzálódik a hőterhelés. Ha azonban a hőtermelés meghaladja a bőrfelületről történő hőveszteség felső határát a magas környezeti hőmérséklet, a páratartalom, az alacsony szélsebesség vagy a ruházat magas párolgási ellenállása miatt, akkor a test maghőmérséklete folyamatosan emelkedik, kialakul a kompenzálatlan hőterhelés.[7]

Ha a test természetes hűtőfolyamatai nem képesek a felesleges hő csökkentésére, az még megfelelő adaptáció mellett is befolyással van a fizikai és kognitív teljesítményre.[8] A tűzoltói beavatkozások során a hőterhelés a makrokörnyezet védőruházaton keresztülhatoló hatásainak, a munkavégzés következtében termelődő belső hő, valamint az izzadság keltette páratartalom hatásainak összegződéséből ered. A fizikai munkavégzés nagy metabolikus hőtermelést eredményez, mivel az izommunkába fektetett energia 70-80%-a hővé alakul át. Ez a hőtermelés nyugalmi helyzetben 70–100 W, közepes intenzitású munkavégzésnél 280–350 W, magas intenzitású terhelés során elérheti az 1000 W-ot.[9] A védőruházatban az izzadással a hőátadás csökken, mivel a szigetelő rétegek evaporációs ellenállásuknak köszönhetően csak korlátozottan engedik át a vízpárát, így a ruha és test közötti légrésben a relatív páratartalom gyorsan eléri azt az értéket, ahol a párolgás és a test hűtése minimálisra csökken. Hűtés hiányában az emelkedő maghőmérséklet kiváltja a verejtékráta további fokozódását, azonban ez már nem képes további hűtőhatást kiváltani, csak a dehidratáció sebességét növeli.[10] A fokozott mértékű folyadékvesztés hatására jelentősen romlanak a hőszabályozási reakciók, ami tovább súlyosbíthatja a hőterhelés hatásait. Ha a tűzoltók már a beavatkozásaikat megelőzően sincsenek megfelelő hidratáltsági állapotban, és a tűzoltás befejezését követően sem fogyasztanak megfelelő mennyiségű és minőségű folyadékot, a kiszáradás számos tünetét tapasztalhatják. A dehidratációról ismert, hogy érinti az aerob és anaerob képességeket, befolyásolhatja a kognitív funkciókat és az euhidratációhoz képest csökkenti a hőtolerancia idejét.

6 Pavlik 2019: 475.
7 Ravanelli–Bongers–Jay 2019.
8 Dickhuth 2019: 229.
9 Cheung–Lee–Oksa 2016.
10 Cheung 2000.

A hőterhelés hatása a motorikus képességekre és a kognitív funkciókra

A tűzoltói beavatkozások a motorikus képességek teljes spektrumát igénylik. Számos kutatási eredmény alátámasztja, hogy a kompenzálatlan hőterhelés és a kapcsoltan fellépő folyadékveszteség hatással lehet a motorikus képességekre. A hőterhelés hatására fellépő erődeficit egyik lehetséges oka a beavatkozások közben elszenvedett sérüléseknek.[11] Miután az erő, a gyorsaság és az állóképesség mind-mind közvetlenül párosíthatók konkrét tűzoltói feladatokhoz, érdemes megvizsgálni a hőterhelés ezekre gyakorolt negatív hatásait. Az erő és az intenzív állóképességi munkavégző képesség egyenes arányban csökken a folyadékveszteség mértékével. Egy közepesen megterhelő aktivitás során tapasztalható 3-4%-os csökkenés a testtömegben magával hozza az izomerő 2%-os, és az intenzív állóképesség akár 10%-os csökkenését is.[12] Ez a teljesítmény-visszaesés is elgondolkodtató, azonban a hőterhelés legnagyobb mértékben az aerob teljesítményre van hatással. Vizsgálatok kimutatták, hogy tűzoltóknál a hőstressz következtében bekövetkező folyadékveszteség a plazmatérfogat akár 15%-os csökkenését eredményezi.[13] A térfogatcsökkenés következtében csökken a verőtérfogat, amit a szervezet a pulzusszám növelésével kompenzál. Ez a kompenzáció azonban nem képes a végtelenségig kielégíteni az izomzat vérellátási igényét, ezért a teljesítmény visszaesik.

A tűzoltókat érő hőhatások nemcsak a kondicionális képességeket, hanem a kognitív és pszichomotoros-koordinációs képességeket is képesek lehetnek negatívan befolyásolni. A test maghőmérsékletének emelkedése negatívan befolyásolhatja a kognitív teljesítményt, ami növeli a hibák kockázatát, és ez tűzoltási helyzetekben kritikus lehet. A kognitív képességek területén a figyelem és az észlelés befolyásolását, a koordinációs képességek közül pedig a térbeli tájékozódó képesség, a mozgás és egyensúly-érzékelés és a komplex reakcióképesség csökkenését okozhatja. Ezen képességek megváltozásának vizsgálata a tűzoltói beavatkozások közben bekövetkező hőterheléssel kapcsolatosan nem túl mélyen kutatott terület.[14] Egy, a témával foglalkozó összefoglaló tanulmány rámutat a korábbi kutatások vegyes, olykor ellentmondásos eredményeire, és kiemeli a további kutatások fontosságát.[15] Biztosnak látszik azonban, hogy a hőstressz kognitív funkciókra gyakorolt hatásai összefüggenek az élettani változásokkal és a külső, belső terheléssel. További kísérletek kimutatták, hogy a munkahelyi feladatvégzés hatékonysága visszaeshet, ha a környezeti hőmérséklet meghaladja a 23 °C-ot.[16] Emellett Schmit és munkatársai[17] arra a következtetésre jutottak, hogy a kognitív funkciók zavart szenvednek, amikor a test maghőmérséklete 39 °C fölé emelkedik. Ez azt sugallja, hogy a tűzoltókat veszélyeztetheti a hőstressz, ami végső soron hatással van arra a képességükre, hogy életeket védjenek meg. Ezért fontos megérteni a hőterhelésnek a tűzoltók kognitív képességeire gyakorolt hatásait.

[11] Smith 2008.
[12] Judelson et al. 2007.
[13] Smith–Manning–petruzzello 2001.
[14] Carlton–Orr 2015.
[15] Thompson et al. 2023.
[16] Cheung–Lee–Oksa 2016.
[17] Schmit et al. 2017.

Kutatások arra a következtetésre jutottak, hogy az olyan megterhelő feladatok, mint az éberség és a figyelem folyamatos fenntartása, a legérzékenyebbek a hőstresszre; ez aggasztó, tekintettel az ilyen feladatok fontosságára a tűzoltásban, a helyzetek összetettségére, amelyeknek a tűzoltó ki van téve, és a nehéz döntésekre, amelyeket meg kell hoznia.[18] Ezzel együtt nem világos, hogy a hőmérséklet pontosan hogyan és milyen mértékben befolyásolja a tűzoltók kognitív képességeit, mivel a kutatások nem reprezentálják teljeskörűen a tűzoltók munkakörülményeit.

Célkitűzés

Jelen kutatás célja az volt, hogy megismerjük a védőruházaton belüli mikroklíma változásainak dinamikáját és hatását a maghőmérsékletre, és ezáltal a folyadékvesztésre. A vizsgálat alapkérdése volt, hogy kialakulhatnak-e hőterhelést előidéző mikroklimatikus tényezők a védőruházatban a beavatkozások kezdeti szakaszában a tényleges tűzoltást megelőzően. Hogyan változik a maghőmérséklet és bőrhőmérséklet, milyen ütemben alakul ki a kompenzálatlan hőterhelés? Van-e lényeges különbség azonos munkavégzés és külső környezeti feltételek mellett védőruházatot viselve és sportruházatban végrehajtott terhelés élettani mutatóiban?

Anyag és módszer

A kutatás során hivatásos tűzoltókat vizsgáltam (n = 10). Adataik a 1. táblázatban találhatók.

1. táblázat: A résztvevők adatai

Résztvevők (n = 10)	**Átlag ± szórás**	**Terjedelem**
Életkor (év)	40,9±7,88	[28–53]
Testmagasság (m)	173,4±6,58	[163–182]
Testtömeg (kg)	69,6±8,04	[58–81]
Testfelszín (m^2)[19]	1,82±0,11	[1,62–1,95]
Testtömegindex (BMI)	23,21±3,07	[19,48–29,04]

Forrás: a szerző szerkesztése

A résztvevők a vizsgálatra megfelelő hidratáltsági állapotban érkeztek, a vizsgálat előtt 24 órával kerülték az alkoholfogyasztást, a 25 °C feletti tartós hőhatást és a kimerítő testmozgást; valamint a vizsgálat előtt 2 órával nem fogyasztottak kávét, teát vagy csokoládét. A résztvevők közül senki sem járt rendszeresen szaunába, és egyikük sem volt kitéve hőhatásnak (> 25 °C) a teszt előtti 24 órában.

[18] Hancock–Vasmatzidis 2003.
[19] Mosteller 1987.

A vizsgálati eljárás

A mérések zárt, klimatizált helyiségben történtek a külső környezeti hatások csökkentése érdekében. (hőmérséklet: 22±1,6 °C páratartalom: 46±12%) A védőruha felvételét megelőzően helyeztem fel a Polar H10 pulzus (Polar Electro Oy, Finland) Core maghőmérséklet (Core, Switzerland) és a belső hőmérséklet és páratartalom szenzort (Ruuvi Innovations, Finland) a rendszeresített 10M gyakorlópóló alá. A póló felvételét követően még egy Kestrel D2 hőmérséklet és páratartalom adatrögzítő szenzort (Kestrel Instruments, USA) is elhelyeztem a védőruházat alá. A védőruházat kabátból, nadrágból és csizmából állt. Légzőkészüléket, sisakot, kámzsát, védőkesztyűt a résztvevők nem viseltek. A mérések folyamán egy esetben a védőruhás és egy esetben a kontrollmérések során a légzési gázok analízise Calibre (Calibre Biometrics, USA) műszerrel történt. A terheléses teszt elliptikus tréneren (Horizon Elite 4000) történt 1-es nehézségi fokozaton 70±5 W terhelés mellett a gyors tempójú járásnak megfelelő 60±5 lépés/perc frekvenciával. A méréseket megelőző tájékoztatás során felhívtam a résztvevők figyelmét az egyenletes tempó tartására. Az észlelt erőfeszítés mértékét (RPE) 20 fokozatú Borg-skálán[20] a következő numerikus-verbális módon értékelték: 6 „minimális terhelés"; 7–8 „nagyon könnyű"; 9 „komfortos"; 10–11 „komfortos, kis erőfeszítés"; 12 „komfortos, közepes erőfeszítés"; 13 „kicsit fárasztó"; 14–15 „megterhelő"; 16–17 „nagyon megterhelő"; 18–19 „extrém terhelés"; 20 „maximális terhelés". Az érzékelt hőérzetet a következő numerikus-verbális horgonyok felhasználásával értékelték: „nagyon hideg"; „hideg"; „hűvös"; „kissé hűvös"; „semleges"; „enyhén meleg"; „meleg"; „nagyon meleg"; „elviselhetetlenül meleg". Az izzadás érzékelt mértékét és izzadás érzését a következő numerikus-verbális horgonyok segítségével értékelték: „nem érzem"; „enyhén izzadok"; „izzadok"; „közepesen izzadok"; „erősen izzadok".

A teszt a védőruházat felvételét követően öt perces ülő helyzetű nyugalmi szakasszal kezdődött a vonulás közbeni terhelés szimulálására. Az öt perc elteltét követően kezdődött a 30 perces egyenletes ellenállással és lehetőleg egyenletes lépésfrekvenciával végrehajtott mérés. A résztvevők minden ötödik perc elteltével közölték az érzékelt erőfeszítés, hőérzet és izzadás értékét. A kontrollcsoport által végzett tesztben megismételtük az előző mérési protokollt, de ezúttal hosszú ujjú és hosszúszárú egyrétegű sportruházatban. A szenzorok közül a külső hőmérséklet és páratartalom szenzor helyett környezeti adatrögzítőt használtam.

A mérések terhelését a szakirodalomban található, az egyes tűzoltást megelőző szerelési feladatok energiaigényét metabolikus egyenértékben (*metabolic equivalent of task,* MET)[21] meghatározó tanulmányok[22] alapján, valamint a hazai tűzoltók fizikai alkalmasságvizsgálatát validáló tanulmány eredményeinek felhasználásával határoztam meg.[23] Egy metabolikus egyenérték (MET) a pihenő helyzetben, ülve felhasznált oxigénmennyiségként definiálható, és 3,5 ml percenkénti és testtömegkilogrammonkénti (ml O_2/kg/min) oxigénfelhasználásnak felel meg. A MET koncepciója egyszerű: a fizikai tevékenységek energiaigényét a nyugalmi anyagcsereérték többszörösével

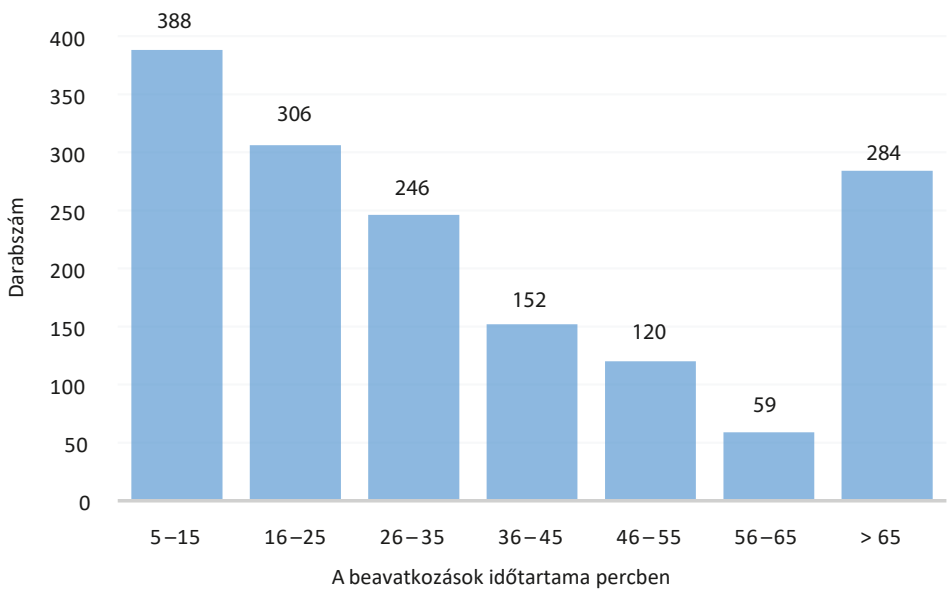
[20] Borg 1982.
[21] Jetté–Sydney–Blümchen 1990.
[22] Dos Santos et al. 2025.
[23] Kanyó – Vásárhelyi-Nagy 2021.

fejezi ki. A releváns szakirodalom szerint a tűzoltó szerelési feladatok energiaigénye 7–10 MET, a hazai tűzoltók fizikai alkalmasságvizsgálatának elvégzéséhez szükséges átlagos érték 13,3 MET. A vizsgálat során a védőruházatban végrehajtott feladatnál az ellipszistréneren mért oxigénfelvételből számítva a teszt energiaigénye átlagosan 9±1 MET egység volt, ami megfelel a szerelési munkák átlagos terhelésének (2. táblázat). Érdekesség, hogy az Egyesült Államokban szabványként alkalmazott NFPA 1582[24] ajánlás által megszabott tűzoltói alkalmassági minimumérték a 12 MET, ami 42 ml maximális oxigénfelvevő képességnek felel meg.

2. táblázat: A tűzoltói feladatok energiaigénye MET-egységben kifejezve

Tevékenység	**Energiaigény metabolikus egységben meghatározva (MET)**	**Relatív oxigénfelvétel (ml O_2/kg/min)**
Lépcsőzés (teher nélkül és terheléssel)	8,1–10,7	28,3–37,4
Létramászás	9,7–11,4	33,9–39,9
Lépcsőzés légzőkészülékkel és külső teherrel	11,1–13,0	38,5–45,5
Tömlőgurítás, fektetés	7,1–9,8	24,8–34,3
Tűzoltás-szimuláció tömlővel	10,1–13,4	35,3–46,9

Forrás: a szerző szerkesztése DOS SANTOS *et al. 2025 alapján*



2. ábra: A tűzesetek felszámolásáig eltelt idő eloszlása
Forrás: a szerző szerkesztése

[24] NFPA 1582 2022.

A mérések időtartamát a fővárosban 2024-ben végrehajtott beavatkozások adataiból készült statisztikák alapján határoztam meg. A beavatkozások elemzésénél jelen tanulmány számára a fővárosi tűzesetek statisztikái szolgáltak alapul. Az események adatai közül kizárólag a beavatkozást igénylő tűzesetek kerültek be a vizsgálatba, a műszaki mentéseket kizártam. A tűzeseti beavatkozások adatai közül a statisztikai torzítás kiküszöbölésére eltávolítottam az elhúzódó (3 óránál hosszabb) és az öt percnél rövidebb eseteket. Az így nyert adatok azt mutatják, hogy az átlagos beavatkozási időtartam, ami a kiérkezéstől a felszámolásig tart, 39 perc, a medián időtartam 29 perc. Az adatokból következik, hogy a tűzeseteknél a vonulás megkezdésétől a felszámolásig védőruhában töltött idő az esetek többségében meghaladja a jelen vizsgálatban alkalmazott 30+5 percet. A beavatkozások időbeni eloszlása jól látható a 2. ábrán.

Eredmények

A statisztikai számításokat JMP 18 szoftverrel végeztem. A bevetési ruhában (BEV) és a sportruházatban végzett kontrollcsoportok (KON) közötti eredmények összehasonlítása kétmintás t-próbával történt a statisztikai szignifikancia szintje $p < 0,05$ volt. A tesztek végén mért maghőmérsékletek (T_c) összehasonlítása kétmintás t-próbával történt. A teszt eredménye, hogy a BEV-csoportban (átlag [M] = 38,36; szórás [SD] = 0,116) és a KON-csoportban (M = 37,99; SD = 0,055) a T_c szignifikáns ($p = 0,010$) különbséget mutattak. A 35. percben mért maximális bőrhőmérsékletek (T_s) BEV- (M = 35,6; SD = 0,565) és a KON-csoportban (M = 31,78 SD = 1,051) a T_s szignifikánsan ($p = 0,00134$) eltérnek. A teszt végén detektált pulzusszámok (HR) esetében a BEV- (M = 163,4; SD = 8,414) és KON- (M = 133; SD = 9,848) csoportok között a statisztikai elemzés jelentős különbséget mutatott ki ($p = 0,0127$). A BEV-csoportban a maghőmérséklet és a ruha–test közötti légrésben mért hőmérséklet (T_{gap}) kapcsolatát Pearson-féle korrelációval vizsgáltam. Az eredmény ($r = 0,7587$) alapján a két változó között erős pozitív kapcsolat fedezhető fel. A mért bőrhőmérséklet és a ruházat alatti légrés hőmérséklete között végzett korrelációs elemzés nagyon gyenge kapcsolatot ($r = 0,2823$) mutatott ki. Az ötperces adatokon alapuló maghőmérséklet-görbék töréspontjának kiszámítása matematikai úton a függvények analízisével történt.

Megbeszélés

A test hőegyensúlya a hőtermelő és hőleadási folyamatok kiegyenlítésének eredménye. Az egyensúly szempontjából fontos tényezők a metabolikus hőtermelés mértéke, a ruházat hővezetési tulajdonságai és a környezeti viszonyok. A bevezetőben kiemeltük azt a tényt, hogy a védőruházat célja a környezetistressz-tényezők hatásának kiküszöbölése vagy csökkentése. A fizikai és kémiai hatások elleni védelem a legtöbb esetben speciális szövetek és azok különböző kezeléseinek alkalmazását jelenti, amelyek a vízpára számára korlátozottan átjárhatók. A megfelelő védelem ezért gyakran csak a test hőegyensúlyának jelentős befolyásolásával érhető el.

A hőáramlást a ruházaton keresztül két tulajdonság határozza meg, a hőszigetelés és a párolgási ellenállás. A hőszigetelés a ruházat hőáramlás, hősugárzás és hővezetés útján történő hőátadásnak való ellenállása, míg a párolgási ellenállás a ruha vízpára-áteresztő képességének mérőszáma. A hőszigetelést a ruha anyagának tulajdonságai, a szövet szerkezete, valamint a szövetrétegek közti levegőréteg határozza meg. Ezek közül a legfontosabb tényező a légrétegek vastagsága. A párolgási ellenállás a vízpára áteresztésének ellenállása, mivel az átvitt hő a bőr felületén elpárolgó és a környezetbe átjutó nedvességhez kötődik. Ennek megfelelően a nedvességátvitelhez kapcsolódó tulajdonságok meghatározóak a párolgási hőcserében. A szövet legfontosabb tulajdonsága a pórusok mérete és a légrétegek vastagsága. Minél kisebbek a pórusok, és minél vastagabbak a légrétegek, annál kisebb lesz az átvitt vízgőz mennyisége, és annál kisebb lesz a hőveszteség.[25]

A tűzoltó védőruházat vízszigetelését a középső rétegben elhelyezkedő mikroporózus membrán végzi. A membránokon kialakuló vízkondenzáció eltömítheti a pórusokat, csökkentheti a gőzáteresztő képességet és ronthatja a porózus membránok teljesítményét. Bebizonyosodott, hogy a porózus membránon lévő folyadék „szennyeződése" csökkenti a membránon keresztüli nedvességdiffúzió sebességét, mivel eltömíti a pórusokat, és ezáltal csökken a nyitott terület.[26] Az elméletet igazolja, hogy a mérések során az átlagos relatív páratartalom a teszt végére meghaladta a 80%-ot (80,64%; SD = 8,59), ami már jelentős kondenzációt váltott ki mind a bevetési ruhán, mind a testen. A ruházat alatti mikroklíma közvetlenül befolyásolja a bőr felületén zajló hőcserét, és jelentősen meghatározza a fiziológiai és pszichológiai reakciókat. A mért adatok szerint az átlagos hőmérséklet a védőruha alatti légrésben a munkavégzés 10. percében már meghaladja a 30 °C-ot és a 65%-os páratartalmat. A két érték az idő múlásával párhuzamosan gyors ütemben növekszik, amit a statisztikai vizsgálat is igazolt.

3. táblázat: Mikroklimatikus viszonyok a védőruházaton belül

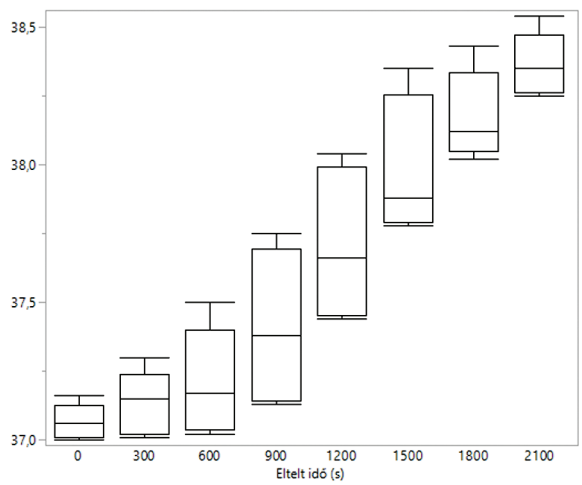
Eltelt idő (min)		5	10	15	20	25	30	35
Hőmérséklet (°C)	Átlag	30,87	31,90	32,71	33,21	33,57	33,75	33,85
	SD	2,17	1,52	1,18	1,08	1,04	1,07	1,03
Páratartalom (RH %)	Átlag	63,05	67,17	71,70	74,07	76,9	78,45	80,95
	SD	7,63	8,79	8,50	9,19	8,49	9,71	9,89

Forrás: a szerző szerkesztése

A mikroklíma levegőjének hőmérséklete és vízgőznyomása szoros összefüggésben áll a viselt ruházat hőmérséklet-visszatartó tulajdonságaival. A félig áteresztő képességű szövetek esetén a vízgőznyomás fokozatosan emelkedik, és ha a beavatkozás elég

[25] Holmér 2006.
[26] Khakpour–Gibbons–Chandra 2021.

hosszú ideig tart, elérheti a telítettségi nyomást (100% relatív páratartalom). A párolgás gátlása miatt bekövetkező csökkent hőcsere miatt a ruházat alatti mikroklíma léghőmérséklete és a bőr hőmérséklete is jelentősen emelkedhet (3. táblázat). Amikor a bőrhőmérséklet megemelkedik, és eléri vagy meghaladja a külső környezet hőmérsékletét, a hőleadás legfontosabb csatornája a párolgás. A szervezet válasza a meleg környezetben a hőegyensúly megtartása érdekében az izzadási ráta megemelése. Mivel a párával részben telített környezet az izzadság további párolgását megakadályozza, a hűtés elégtelenné válik, és a maghőmérséklet emelkedni kezd. A 3. ábrán látható, hogy a résztvevők maghőmérséklete a teszt kezdetekor viszonylag egységesen a 37–37,3 °C sávban mozgott. A terhelés megkezdésével az egyes résztvevőknél eltérő ütemben kezdődött meg a maghőmérséklet emelkedése, de az ábrán a 12. perctől ugrásszerű növekedés figyelhető meg. A 10–25 perc közötti intervallumban tapasztalt maghőmérséklet-emelkedések nagyobb szórását az egyes résztvevők egyéni reakciója, edzettsége, esetleges hőakklimatizációs státusza befolyásolta. A teszt végső fázisában mért maghőmérsékletek egyre kisebb szórással 38,3–38,5 °C között alakultak.



3.ábra: A védőruházatban mért maghőmérséklet változása
Forrás: a szerző szerkesztése

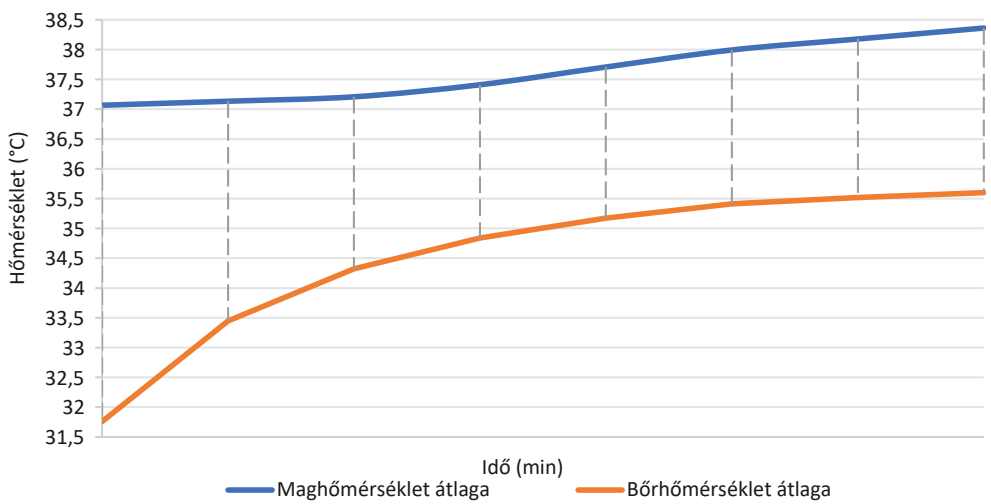
Kompenzálatlan hőterhelés akkor következik be, amikor a test felületéről a hőt az izzadás nem képes olyan sebességgel elvezetni, amilyen ütemben azt termeli. Ilyen esetekben a fokozott izzadás ellenére a hőleadás hatékonysága visszaesik, és nem képes a folyamatos testhőemelkedést megakadályozni. A kompenzálatlan hőterhelést több módon is detektálhatjuk. A legegyszerűbb módszer a maghőmérséklet növekedésének ütemét vizsgálva megállapítani, mikor éri el és haladja meg a 0,03 °C percenkénti emelkedést. A kísérletben részt vevőknél ez átlagosan 15 perc elteltével, de 20 percet nem elérve következett be, míg a kontrollcsoport eredményei ezt a jelenséget nem igazolták. A 4. táblázatban látható eredmények rávilágítanak arra, hogy az átmenet a két állapot között a maghőmérséklet ugrásszerű emelkedésével jár együtt.

4. táblázat: A maghőmérséklet növekedésének üteme a védőruhás csoportnál

Eltelt idő (s)	300	600	900	1200	1500	1800	2100
Maghőmérséklet változása (°C/5 perc)	0,068	0,074	0,202	0,298	0,286	0,184	0,184
A maghőmérséklet percenkénti változása ΔT(°C/perc)	0,0136	0,0148	0,0404	0,0596	0,0572	0,0368	0,0368

Forrás: a szerző szerkesztése

A kompenzálatlan hőterhelésre következtethetünk a maghőmérsékleti görbék töréspontjából is. Az egyes maghőmérsékleti grafikonokon az állapotváltozást jelző töréspontot egy eset kivételével valamennyi görbén sikerült kimutatni a görbék matematikai elemzésével. A számítások kimutatták a második derivált előjelváltását, tehát sz inflexiós pont létezését. Ez a matematikai töréspont erős korrelációt mutatott (r = 0,8695) a 0,03 °C/perc hőmérséklet-emelkedést jelző adatokkal. Annál a résztvevőnél, ahol a töréspont matematikailag nem volt kimutatható, feltételezhetően a meglévő hőakklimatizáció miatt, a szervezet nem lépett át a kompenzálatlan hőterhelési szakaszba. További kutatást igényel az, hogy a maghőmérsékletet és a bőrhőmérsékletet ábrázoló görbék közötti távolság (4. ábra) változásából kimutatható-e a hőkompenzációs átmenet.



4. ábra: A maghőmérséklet és a bőrhőmérséklet összefüggései
Forrás: a szerző szerkesztése

Összegzés

A fenti elemzések alapján megerősíthető az a feltevés, miszerint a tűzoltók hőterhelését jelző kompenzációs pontot a közvetlen tűzoltási feladatokat megelőzően az előkészítő szerelési munkák alatt is átlépheti a szervezet. Az eredmények tükrében igazolható a feltételezés is, hogy már a beavatkozások kezdeti szakaszában olyan mikroklimatikus viszonyok alakulhatnak ki a védőruházatban, amelyek kompenzálatlan hőterhelés kialakulásához vezethetnek. Az adatok azt mutatták, hogy a védőruházaton belül a teszt végén az átlagos légréshőmérséklet 33,58 °C, (SD 1,03) és a relatív páratartalom 80,95% (SD 9,89) volt.

Kutatási kérdés volt az is, hogy közepes intenzitású fizikai munkavégzés során tűzoltó bevetési védőruházatban milyen időtartam alatt éri el a szervezet a kompenzálatlan hőterhelés zónáját. A mérési eredmények tükrében látható, hogy a bevetési védőruhát viselő személyeknél a kompenzálatlan hőterhelést jelző markerek jellemzően a 15. és 18. perc között jelentek meg. A statisztikai elemzés adataiból kiderül, hogy azonos külső terhelés mellett a kontrollcsoportban sem a maghőmérséklet, sem a bőrhőmérséklet, sem a terhelés mértékét jelző pulzusszám nem éri el a bevetési ruhás értékeket. A bevetési ruhában (BEV) és a sportruházatban végzett (kontroll, KON) 35 perc időtartamú 9±1 MET-egységben megszabott terheléses vizsgálaton a csoportok közötti eredmények alapján a két csoport maghőmérséklet (Tc) értékei között jelentős eltérés mutatkozott. BEV-csoportban (átlag [M] = 38,36; szórás [SD] = 0,116) és a KON-csoportban (M = 37,99; SD = 0,055) a Tc-értékek szignifikáns ($p = 0,010$) különbséget mutattak. A teszt végén detektált pulzusszámok (HR) esetében a BEV- (M = 163,4; SD = 8,414) és KON- (M = 133; SD = 9,848) csoportok között a statisztikai elemzés szintén jelentős különbséget mutatott ki ($p = 0,0127$).

A vizsgálat eredményei támpontot adhatnak a további kutatásokhoz, amelyek arra irányulnak, hogy a test maghőmérsékletének emelkedése milyen mértékű folyadékvesztéssel jár, és ez milyen hatással van a tűzoltók fizikai és kognitív teljesítményére.

A kutatás korlátai

A vizsgálat limitációja, hogy a minta mérete és ezzel a rendelkezésre álló adatok mennyisége nem elegendő a minőségi statisztikai adatelemzéshez és az eredmények széles körű alkalmazásához. Továbbá a minta összetétele nem reprezentálja teljeskörűen a tűzoltók demográfiai eloszlását. A kutatás későbbi szakaszaiban szükséges a minta méretének növelése és a résztvevők véletlenszerű kiválasztása.

Felhasznált irodalom

Borg, Gunnar A. (1982): Psychophysical Bases of Perceived Exertion. *Medicine & Science in Sports & Exercise,* 14(5), 377–381. Online: https://doi.org/10.1249/00005768-198205000-00012

Carlton, Andrew – Orr, Robin Marc (2015): The Effects of Fluid Loss on Physical Performance: A Critical Review. *Journal of Sport and Health Science,* 4(4), 357–363. Online: https://doi.org/10.1016/j.jshs.2014.09.004

Cheung, Stephen S. – Lee, Jason K.W. – Oksa, Juha (2016): Thermal Stress, Human Performance, and Physical Employment Standards. *Applied Physiology, Nutrition, and Metabolism,* 41(2), 148–164. Online: https://doi.org/10.1139/apnm-2015-0518

Cheung, Stephen S. et al. (2000): The Thermophysiology of Uncompensable Heat Stress. Physiological Manipulations and Individual Characteristics. *Sports Medicine,* 29(5), 329–359. Online: https://doi.org/10.2165/00007256-200029050-00004

Dickhuth, Hans-Hermann (2005): Táplálkozás, hő-, víz-, elektrolit-háztartás és a testi aktivitás. In *Sportélettan, sportorvostan.* Budapest: Dialóg Campus.

Dos Santos, Lopes Marcel et al. (2025): The Metabolic Demand of Firefighting: A Systematic Review. *Physiologia,* 5(2), 12. Online: https://doi.org/10.3390/physiologia5020012

Hancock, P. A. – Vasmatzidis, I. (2003): Effects of Heat Stress on Cognitive Performance: The Current State of Knowledge. *International Journal of Hyperthermia,* 19(3), 355–372. Online: https://doi.org/10.1080/0265673021000054630

Holmér, Ingvar (2006): Protective Clothing in Hot Environments. *Industrial Health,* 44(3), 404–413. Online: https://doi.org/10.2486/indhealth.44.404

Horváth Lilla (2023): A tűzoltó egyéni védőeszközök fejlesztési lehetőségei ergonómiai szempontok alapján. In Padányi József – Gőcze István (szerk.): *Húsz év a katonai műszaki tudományok szolgálatában*. Budapest: Ludovika, 71–79.

Jetté, M. – Sydney, K. – Blümchen, G. (1990): Metabolic Equivalents (METS) in Exercise Testing, Exercise Prescription, and Evaluation of Functional Capacity. *Clinical Cardiology,* 13(8), 555–565. Online: https://doi.org/10.1002/clc.4960130809

Judelson, Daniel A. et al. (2007): Hydration and Muscular Performance: Does Fluid Balance Affect Strength, Power and High-Intensity Endurance? *Sports Medicine,* 37, 907–921. Online: https://doi.org/10.2165/00007256-200737100-00006

Kanyó Ferenc – Vásárhelyi-Nagy Ildikó (2021): A beavatkozó tűzoltói állomány kompetencia alapú fizikai állapotfelmérése. *Védelem Tudomány,* 6(1), 204–217. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13455

Khakpour, Ariana – Gibbons, Michael – Chandra, Sanjeev (2021): Effect of Moisture Condensation on Vapour Transmission Through Porous Membranes. *Journal of Industrial Textiles,* 51(2_suppl), 1931–1951. Online: https://doi.org/10.1177/15280837211014239

Kutasi Csaba (2025): A tűzoltó-védőruházatok főbb jellemzői. *Magyar Textiltechnika,* 73(2), 16–22. Online: https://tmte.hu/wp-content/uploads/2025/05/MTT2025_2_16_Tuzolto.pdf

Mosteller, Randhawa D (1987): Simplified Calculation of Body Surface Area. *New England Journal of Medicine,* 317(17), 1098. Online: https://doi.org/10.1056/nejm198710223171717

NFPA 1582 Standard on Comprehensive Occupational Medical Program for Fire Departments (2022). NFPA. Online: www.nfpa.org/codes-and-standards/nfpa-1582-standard-development/1582

Pántya Péter (2018): A Katasztrófavédelem beavatkozó hatékonyságának fejlesztése a tűzoltósági területen. *Hadmérnök,* 13(Különszám), 109–144. Online: www.hadmernok.hu/180kofop_07_pantya.pdf

Pavlik Gábor (2019): *Élettan-sportélettan*. Budapest: Medicina.

Ravanelli, Nicolas – Bongers, Coen – Jay, Ollie (2019). The Biophysics of Human Heat Exchange. In Périard, Julien – Racinais, Sébastien (szerk.) *Heat Stress in Sport and Exercise*. Cham: Springer, 29–43. Online: https://doi.org/10.1007/978-3-319-93515-7_2

Schmit, Cyril et al. (2017): Cognitive Functioning and Heat Strain: Performance Responses and Protective Strategies. *Sports Medicine,* 47,1289–1302. Online: https://doi.org/10.1007/s40279-016-0657-z

Smith, Denise L. – Manning, T. – Petruzzello, S. (2001): Effect of Strenuous Live-Fire Drills on Cardiovascular and Psychological Responses of Recruit Firefighters. *Ergonomics,* 44(3), 244–254. Online: https://doi.org/10.1080/00140130121115

Smith, Denise L. et al. (2008): *Firefighter Fatalities and Injuries: The Role of Heat Stress and PPE*. Champaign, IL: Firefighter Life Safety Research Center, Illinois Fire Service Institute, University of Illinois at Urbana-Champaign. Online: www.fsi.illinois.edu/documents/research/FFLSRC_FinalReport.pdf

Thompson, Catherine et al. (2023): Do Extreme Temperatures Affect Cognition? A Short Review of the Impact of Acute Heat Stress on Cognitive Performance of Firefighters. *Frontiers in Psychology,* 14. Online: https://doi.org/10.3389/fpsyg.2023.1270898

Vitrai József (2021): Cikkismertetés: A magas hőmérséklet egészségkockázata. *Egészségfejlesztés,* 62(4), 86–91. Online: https://doi.org/10.24365/ef.v62i4.7242

HADMÉRNÖK
KATONAI LOGISZTIKA

21. évfolyam (2026) 1. szám 167–188.
DOI: 10.32567/hm.2026.1.11

Szajkó Gyula,[1] Pap Andrea,[2] Gulyás György,[3] Fábos Róbert[4]

A katonai logisztika alapképzési szak szakharcászati gyakorlatának tapasztalatai és újszerű elemei az RSOM-műveletek tükrében

Experiences and New Elements of the Military Logistics Bachelor's Tactical Training in the Context of RSOM Operations

Absztrakt

Az orosz–ukrán ellentét, majd a kibontakozó fegyveres konfliktus megváltoztatta a NATO és az európai államok a térség biztonsági környezetéről alkotott álláspontját. A szövetség az alkalmazandó erők növelése mellett egyre nagyobb figyelmet fordít a reception, staging, onward movement (RSOM – fogadás, állomásoztatás, előrevonás) képességek kialakítására, annak érdekében, hogy biztosítsa a haderők gyors és zökkenőmentes bevethetőségét az európai hadszíntéren. A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp és Katonai Közlekedési Tanszék[5] oktatói számára

[1] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: szajko.gyula@uni-nke.hu
[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: pap.andrea@uni-nke.hu
[3] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: gulyas.gyorgy@uni-nke.hu
[4] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: fabos.robert@uni-nke.hu
[5] 2017-es szervezeti megnevezés, jelenleg NKE HHK Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék (HPKKT).

világossá vált, hogy a logisztikai alapképzésben részt vevő honvéd tisztjelöltek felkészítése során nagy hangsúlyt kell helyezni az RSOM-hez kapcsolódó feladatokra és az azokban bekövetkezett változásokra is. A tanulmány célja, hogy bemutassa a katonai logisztika alapképzési szak szakharcászati gyakorlatának keretei között megvalósított RSOM-orientált kiképzési elemeket és azok tapasztalatait. A szerzők kitérnek az alkalmazott módszertanra, az újszerű gyakorlati megoldásokra, valamint arra, miként segítik ezen elemek a honvéd tisztjelöltek gyakorlatorientált felkészítését. Ezek a feladatok a későbbiekben a beosztásuk betöltésekor is megjelenhetnek mind országvédelmi, mind válságreagáló műveletekben. Ezért is fontos, hogy a kar szervezeti eleme és a kiképzést támogató katonai szervezetek folytassák az együttműködést, valamint az oktatók fejlesszék a kiképzési programot, amely igazodik a biztonságpolitikai helyzetben bekövetkezett változásokhoz.

Kulcsszavak: RSOM-műveletek, felkészítés, törzsmunka, szakharcászati gyakorlat, új elgondolások

Abstract

The Russian–Ukrainian confrontation, followed by the unfolding armed conflict, has significantly altered the standpoint of NATO and European states on the security environment of the region. In addition to increasing applicable forces, the Alliance is placing growing emphasis on developing RSOM (Reception, Staging, Onward Movement) capabilities in order to ensure the rapid and seamless deployment of troops across the European theatre. For the lecturers of Department of Supply, Finance and Military Transportation, Faculty of Military Science and Officer Training of Ludovika University of Public Service, it has become clear that greater emphasis must be placed on RSOM-related tasks and their changes in the training of graduating cadets who study in the military logistics BSc programme. This article aims to present the RSOM oriented training elements and their practical implementation within the framework of tactical field exercises conducted in the programme. The authors examine the applied methodology, innovative practical approaches, and how these elements contribute to the practice-based preparation of cadets. These tasks can appear in the professional duties of officers, both in national defence and crisis response operations, therefore it is very important to maintain the cooperation between the organisational units of the faculty and the supporting military, and for instructors to refine the training programme to reflect changes in the security environment.

Keywords: RSOM operations, training, staff work, tactical field exercise, new approaches

Bevezetés

A katonai műveletek végrehajtásakor a parancsnokok számára meghatározó, hogy a személyek a hadfelszerelésekkel együtt az előre meghatározott időre, a megfelelő minőségben, valamint mennyiségben érkezzenek meg a kijelölt célterületre. A NATO és az európai tagállamok vezetőinek ilyen irányú elvárása az orosz–ukrán fegyveres konfliktus kibontakozását követően fokozódott. A szövetség kiemelt figyelmet fordít

az erők növelése mellett az RSOM[6]-képességek kialakítására annak érdekében, hogy biztosítsa az európai hadszíntéren a haderők gyors és zökkenőmentes bevethetőségét. E folyamat elősegítése érdekében 2016-tól a katonai szövetség keleti határain lévő tagállamaiban (köztük Magyarországon is) NATO Erőket Integráló Elemeket (NATO Force Integration Unit, NFIU) hoztak létre. Legfontosabb feladatuk, hogy elősegítsék a többnemzeti kötelékek gyors és hatékony átcsoportosítását, valamint támogassák a kollektív védelemmel kapcsolatos tervezési munkálatokat.[7] Ennek keretében az NFIU állománya adatokat gyűjt például az érintett országok befogadó nemzeti támogatás (BNT) keretében nyújtható szolgáltatásairól és korlátozásairól, valamint a földrajzi környezet hatásairól, amelyek befolyásolhatják a csapatok sikeres mozgatását az európai hadszíntéren.

Az elmúlt nyolc évben ráadásul több olyan felkészítést és kiképzést hajtott végre a NATO (például az Egyesült Államok Szárazföldi Erőinek Európai Parancsnoksága által vezetett Saber Guardian 2017 és 2019 elnevezésű, összhaderőnemi műveletnek megfelelő gyakorlatokat), amelyek fő célja a hiteles, kollektív védelmi képességek demonstrálása volt a fekete-tengeri régióban. Ezek az egymással összefüggő gyakorlatsorozatok az erők felvonultatásából, éleslövészetekkel egybekötött, terepen végrehajtott harcászati manőverekből, valamint számítógéppel támogatott törzsvezetési mozzanatokból tevődtek össze. A Magyar Honvédség (MH) – a saját csapatok részvételén túl – BNT keretében konvojtámogató központokat is működtetett, hogy biztosítsa az ország területére érkező szövetséges alakulatok biztonságos továbbhaladását. A gyakorlatok tapasztalatai azt mutatták, hogy a haderők hatékony mozgatásához, a tagországok közötti magas fokú együttműködésre, koordinációra, valamint az infrastruktúrák alkalmazhatóságára van szükség. Ennek érdekében a NATO Szövetséges Haderők Európai Főparancsnoksága (SHAPE) megfogalmazta azokat a képességkövetelményeket[8] is, amelyeket szükséges biztosítani (Európában) a tranzitországoknak az erők sikeres átvonulásához és felvonultatásához.

A HPKKT oktatói számára világossá vált, hogy a logisztikai alapképzésben részt vevő honvéd tisztjelöltek kiképzése és oktatása során nagy hangsúlyt kell helyezni az RSOM-műveletekhez kapcsolódó feladatokra és az azokban bekövetkezett változásokra is. Ennek érdekében újszerű gyakorlati megoldásokat vezettünk be, hogy ezzel segítsük a honvéd tisztjelöltek gyakorlatorientált felkészítését. A cikkünkben bemutatjuk az RSOM-feladatokat, az általunk kialakított képzés programját, majd a honvéd tisztjelölti kérdőívek alapján elemezzük a kiképzés eredményességét, bízva abban, hogy az egyetem más szervezeti elemei is tudják hasznosítani a tanulmányban szereplő újszerű elgondolásokat.

[6] Az RSOM-műveletek legfontosabb célja, hogy a feladatok végrehajtására kijelölt csapatok az összhaderőnemi parancsnok elvárásainak megfelelően (elérve a teljes műveleti képességet) érkezzenek meg a kijelölt célterületre. Venekei–Szajkó 2020.

[7] Magyar 2022.

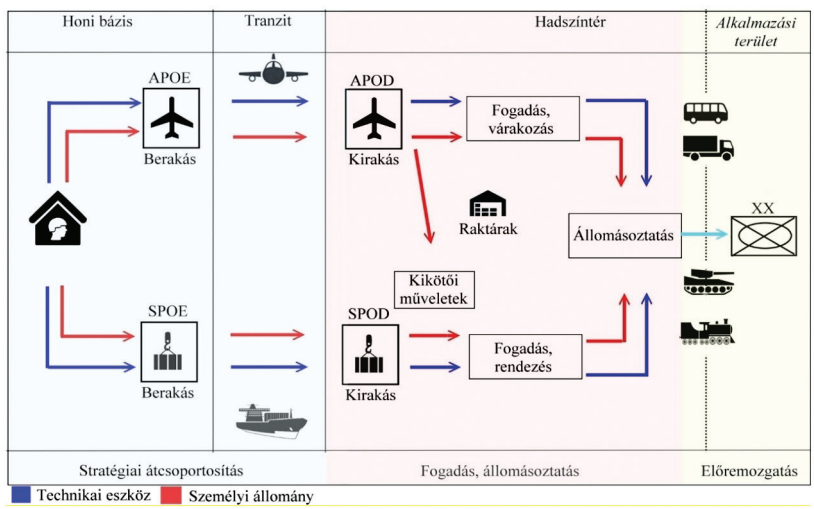
[8] Ezt a NATO SHAPE 2024 írja elő.

Az RSOM-műveletek lényege az erők sikeres mozgatásában

Az RSOM-műveletekkel kapcsolatos eljárásrendeket, feladatokat a NATO Katonai Bizottságának 319/3-as számú határozata (MC-319/3)[9] 82. és 83. paragrafusai, az AJP-4[10] doktrína AJP-3.13 és az ATP-3.13.1 NATO[11] szabvány tartalmazza részletesen. A dokumentumok alapján az RSOM-műveletek célja, hogy a hadműveleti feladatok végrehajtására kijelölt erők az összhaderőnemi parancsnok követelményei szerint a megfelelő időben és állapotban érkezzenek meg a műveleti területre úgy, hogy hatékony támogatásukkal a csapatok elérjék a teljes műveleti képességet. Ezzel összefüggésben az RSOM műveleteit alapvetően két nagy csoportra lehet osztani:

- a csapatok támogatásával, ellátásával kapcsolatos tevékenységek;
- és az erők mozgatásával, szállításával kapcsolatos feladatok.

A támogatással összefüggő feladatokat úgy kell megtervezni és megszervezni, hogy lehetőség szerint magukban foglalják az erők integrálását is (RSOM-I),[12] amely hadműveleti területen az összhaderőnemi parancsnok felelőssége.[13] Az erők mozgatásakor figyelembe kell venni továbbá azt a követelményt, hogy a stratégiai szintű (a csapatok a honi területről a hadszíntérre történő) átcsoportosítások végrehajtásáért a nemzetek felelősek. Ebből következik, hogy az RSOM-műveletek alapvetően az erők hadműveleti szintű mozgatására, szállítására, valamint integrálásának, telepítésének és fenntartásának biztosítására irányulnak a műveleti területen, amelyeket az 1. ábra szemléltet.

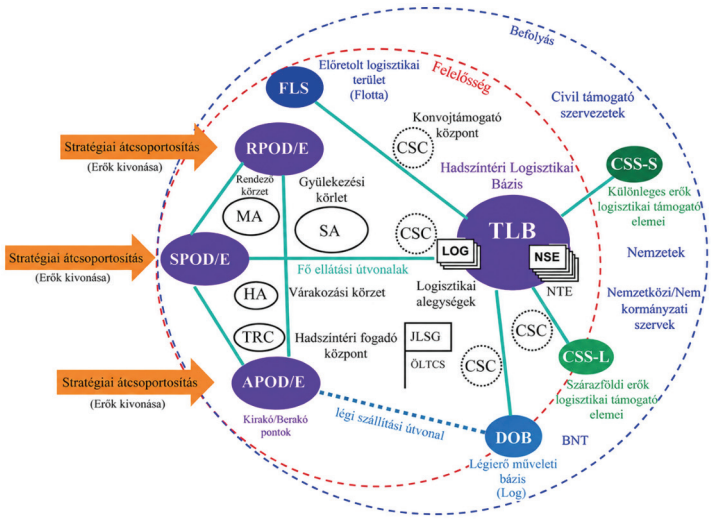


1. ábra: RSOM-műveletek

Forrás: NATO Standardization Agency 2018 és Venekei–Szajkó 2020: 26

[9] MC-319/3 Principles and Policies for Logistics, NATO Military Commitee, Brussels, Belgium, 2014.
[10] NATO Standardization Agency 2025.
[11] NATO Standardization Agency 2014.
[12] *Reception, staging, onward movement and integration.*
[13] Venekei–Szajkó 2020.

Az RSOM-műveletek tulajdonképpen több elemből álló, összefüggő, az Összhaderőnemi Logisztikai Támogató Hálózat (JLSN)[14] részeként értelmezhetők, amelynek összetevőit a 2. ábra mutatja be.



2. ábra: Az Összhaderőnemi Logisztikai Támogató Hálózat felépítése
Forrás: NATO Standardization Agency 2018 és Venekei–Szajkó *2020: 27*

A hálózatba integrált RSOM-elemek legfontosabb feladatai a következők:

- Fogadás: magában foglalja az erők eljuttatását a (tengeri, légi és szárazföldi) kirakó állomásokról a hadszíntéri fogadó központba (TRC),[15] a várakozási (HA),[16] valamint a gyülekezési vagy rendező körzetbe (MA);[17] a folyamatokat biztosító létesítmények, infrastruktúrák felkészítését az alkalmazásra, az adminisztrációhoz kapcsolódó tevékenységeket, beleértve a személyi állomány eligazítását.
- Állomásoztatás: az ide tartozó elemeken keresztül valósul meg a csapatok (a hadszíntérre érkező személyi állomány és a haditechnikai eszközök) alegységekbe, egységekbe rendezése, integrációja annak érdekében, hogy az előrevonásuk sikeresen végrehajtható legyen.
- Előremozgatás: tartalmazza a személyi állomány és a haditechnikai eszközök mozgatási-szállítási feladatait a gyülekezési körletből (SA[18]) az alkalmazási területre. Az eredményes végrehajtás érdekében különböző szállítási módszereket is lehet alkalmazni, amelyek közé tartozhat a BNT keretében biztosítható szolgáltatások igénybevétele is.[19]

[14] Joint Logistic Support Network.
[15] *Theatre reception centre.*
[16] *Holding area.*
[17] *Marshalling area.*
[18] *Staging area.*
[19] NATO Standardization Agency 2014: 13.

Magyarország mint tranzitország a már korábban említett „Saber Guardian 2017" gyakorlatsorozat keretében (a saját erők részvétele mellett) részt vállalt a csapatok előremozgatásában is.

A szakharcászati gyakorlat létrehozásának okai

2017. április 19-én a Magyar Honvédség Vezérkar Főnöke kiadta a 144/2017. számú parancsát a „Saber Guardian 2017" (SAGN17) nemzetközi gyakorlat és kapcsolódó nemzeti gyakorlatok előkészítéséről, valamint a „Saber Guardian 2017" gyakorlattal kapcsolatos nemzeti támogatási feladatok végrehajtásáról. Ebben a parancsban az RSOM-műveletek sikeres lebonyolítása érdekében kijelölte a Magyar Honvédség Logisztikai Központot (MH LK) mint illetékes szervezetet többek között:

- a Magyarország területén áthaladó, illetve Magyarország területén különböző kiképzési tevékenységet végrehajtó külföldi nemzetek haderőire vonatkozóan a valós logisztikai támogatás tervezésének és szervezésének végrehajtására, továbbá ugyanezen erők gyakorlatának valós támogatására;
- a SAGN17 gyakorlat végrehajtása érdekében az országon áthaladó, illetve kiképzési tevékenységet végrehajtó nemzetek fegyveres erőinek nyújtott BNT részeként, a megvalósuló mozgásirányítási, közlekedés, hadtáp, haditechnikai és katonai elhelyezési támogatási feladatok irányítása érdekében, RSOM-támogató parancsnokság működtetésére az MH LK Művelet Vezető Központ bázisán;
- az átcsoportosítások MH szintű közlekedési koordinációs feladataira és a szükséges útvonalengedélyek, úthasználati díjmentességek kiadásának biztosítására, valamint a be- és kirakóhelyek közlekedési támogatására;
- CSC[20] megalakítására és működtetésére;
- a ki- és visszatelepülések idején a felelősségi körébe tartozó mértékben a mozgásirányítási és közlekedéstámogatási feladatok megszervezésére.[21]

A fenti parancsnak megfelelően az MH LK parancsnoka a 62/2017-es parancsában elrendelte Budapest helyőrségben, az MH LK objektumában az RSOM Parancsnokság felállítását, valamint az MH Katonai Közlekedési Központ (MH KKK) részére, hogy alakítson meg és működtessen egy Mozgás Koordináló Központot (MCC[22]) az alábbi feladatokkal:[23]

- a mozgások tervezése és koordinálása;
- a szállítási igények nyilvántartása, kezelése;
- az áthaladáshoz kijelölt útvonalak szemrevételezése, a gyorsforgalmi utakat üzemeltető polgári szervezetekkel az együttműködés kiépítése, majd a feladatok tisztázása;

[20] CSC, *convoy support center* (konvojtámogató központ).
[21] 144/2017 HVKF parancs.
[22] MCC, *movement coordination center.*
[23] Pete 2019.

- a vasúti forgalom zavartalan lebonyolításának biztosítása és a hatékony koordinációt a civil szervezetekkel (a MÁV Zrt. és DB vasúttársaságokkal, Rail Cargo Hungaria Zrt. fuvarozó vállalattal, a Schenker Kft. szállítmányozóval);
- a légi (Budapest Liszt Ferenc Nemzetközi Repülőtér) szállítással érkező erők fogadásával és támogatásával kapcsolatos feladatok végrehajtása a repteret üzemeltető vállalat bevonásával;
- a forgalomszabályozáshoz és kíséréshez a személyek és eszközök kijelölése, részükre a vezetési és irányítási feladatok ellátásához megfelelő infokommunikációs eszközök biztosítása;
- őr- és biztosító alegységek kijelölése és felkészítése az átvonuló csapatok részéről felmerülő őrzésvédelmi igények teljesítéséhez.

Az MH LK-hoz rendelt további RSOM- és BNT-feladatok végrehajtásával kapcsolatban az MH Anyagellátó Raktárbázis (MH ARB) részére feladatul szabta a CSC megalakítását és üzemeltetését, amelynek az áthaladó oszlopok részére valós támogatást nyújtó eleme az MH Bakony Harckiképző Központ bázisán, míg a támogatást végrehajtó állománya az MH KKK Közlekedési Anyagraktár objektumába települt.[24]

A CSC működtetéséhez az LK parancsnoka meghatározta – a NATO-szabványoknak megfelelően – azokat a feltételeket, amelyekhez igazodni kellett az erők sikeres támogatása érdekében. A telepítéshez kapcsolódó követelmények és feladatok az alábbi területekre és elemekre vonatkoztak:

- vezetés és irányítás megfelelő biztosításához kiképzett személyi állomány kijelölése és az infokommunikációs hálózat kiépítése, üzemeltetése;
- a betartandó biztonsági és egyéb rendszabályok kidolgozása, majd azok szükséges mértékű ismertetése a központhoz beérkező erők részére;
- a csapatok elhelyezéséhez infrastruktúra és megfelelő szolgáltatás kialakítása (200–700 fő/nap befogadására);
- tábori hajtóanyagraktár telepítése, majd üzemeltetése (75 000 l/nap hajtóanyag-feltöltési és kiadási kapacitással);
- a tábor területén forgalomszabályzás és ellenőrző áteresztő pontok felállítása, valamint működtetése;
- az egészségügyi ellátás megszervezése és biztosítása;
- műszaki szaktevékenység szükség szerinti elvégzése a tábor kiépítéséhez, valamint az őr- és biztosító alegységek tevékenységének vezetése, irányítása;
- javító, karbantartó, vontató kapacitás biztosítása;
- a konvojkísérő (Mozgáskoordináló Központ alárendeltségében feladatot ellátó) állomány ellátása;
- koordináció és együttműködés kiépítése a kijelölt hatóságokkal az erők továbbmozgatása, előremozgatása érdekében.[25]

A HPKKT oktatóiként néhány napig megfigyelőként rész vehettünk a megalakított RSOM Parancsnokság munkájában. Több napot eltöltöttünk az MCC és a CSC bázisán,

[24] 62/2017 MH LK PK parancsa.
[25] Kolonics 2018.

ahol figyelemmel kísértük az ott folyó munkát, megtapasztalhattuk a felmerülő problémákat és a megoldási lehetőségeket. A megfigyeléseink alapján világossá vált, hogy azok a tapasztalatok, amelyeket ott gyűjtöttünk, feltétlenül be kell hogy építsük a honvéd tisztjelöltek oktatásába, hiszen az ilyen jellegű feladatok a jövőben fokozottan jelentkezni fognak az MH-ban, és ezekre a leendő tiszteket fel kell készíteni, valamint jól illeszkedik az akkoriban és a mai napig végrehajtott más gyakorlatainkhoz.

Az egyetemi szakharcászati gyakorlat tervezése során figyelembe vettük az érvényben lévő, az RSOM-műveletekkel kapcsolatos NATO- és hazai dokumentumokat, valamint a magyarországi éles végrehajtásból származó tapasztalatokat is. A honvéd tisztjelöltek gyakorlatorientált felkészítése érdekében továbbá törekedtünk arra, hogy valóságos környezethez igazodó szcenáriókat és incidenslistákat állítsunk össze.

Az első gyakorlatunkat 2017 őszén hajtottuk végre a friss tapasztalatok alapján, ennek időtartama 5 nap volt, amely időtartam a mai napig változatlan. A helyszín akkor még megosztott volt Táborfalva, valamint a Zrínyi Miklós Laktanya és Egyetemi Campus között. Az első napon a kiutazás után a honvéd tisztjelöltek felkészítésen vettek részt, ahol rendszereztük számukra a szükséges ismereteket. Az MH KKK által biztosított mentoroktatók bemutatták a SAGN17 valós végrehajtásának mozzanatait, az RSOM Parancsokság és alárendeltjeinek helyét, szerepét, tevékenységét a tényleges végrehajtásban. A honvéd tisztjelöltek gyakorlatunk 2. napján készítették el a CSC telepítésének szemrevételezési tervét, majd hajtották végre a tényleges szemrevételezést a számukra kijelölt területen. Visszautazás után a 3. nap feladata volt a CSC elhelyezési körletének megtervezése a korábban ismertetett valós állománytábla és az MH LK 62/2017-es tervezési parancsának alapadatai alapján. Ezt az elgondolásukat a honvéd tisztjelölteknek csoportosan, elöljárói jelentés alapján be kellett mutatniuk a gyakorlat vezető állományának. A 4. napon a honvéd tisztjelölteket három csoportra osztottuk a dinamikus szakasz végrehajtása érdekében. Egy csoport lett az RSOM Parancsnokság, a második az MCC, harmadik a CSC, amelyek időben eltolt incidensek alapján szimulálták a szervezeti elemek egy napi tevékenységét a már korábban említett mentoroktatók segítségével. A feladatok között szerepeltek közúti konvojok áthaladása, vasúti szerelvények érkezése hazánkba, légi szállítás, közúti baleset a kijelölt útvonalakon, gépjármű-meghibásodások a menetoszlopokban, eszközmeghibásodás a CSC állományában. Ezek elvégzéséhez hálózatba kötött számítógépes rendszert telepítettünk a kidolgozói helyiségbe, amelyeken keresztül valósult meg a három elem és a gyakorlatvezető közötti kommunikáció. Az informatikai támogatás volt az oka annak, hogy nem Táborfalván hajtottuk végre a teljes gyakorlatot, hanem részben az egyetemen, mivel a bázison még nem tudták biztosítani számunkra a feltételeket. Az évek során ez a probléma megoldódott, így most már – amennyiben rendelkezésünkre áll az objektum – a teljes időtartamban Táborfalvára települünk. Az 5. nap a gyakorlat zárása, amelynek fő mozzanata a hallgatók előző napi tevékenységének jelentése volt, abban a formában és tartalommal, ahogy az a valóságban is megtörtént a SAGN17 gyakorlaton napi szinten a váltások részéről.

Az azóta eltelt években az alapkoncepció, így a végrehajtás időtartama, a levezetés rendje alapjaiban nem változott. A végrehajtás helyszíne mára Táborfalva, mivel a két helyen történő megosztás nem vezetett jobb eredményre. Sokkal hatékonyabban tudtak a hallgatók dolgozni, ha a megszokott napi életükből rövid időre kimozdítottuk

őket, és külső hatásoktól mentesen tudtak a feladatukra koncentrálni. Az incidenseket folyamatosan frissítettük annak érdekében, hogy a lehető legjobban közelítsenek a valóságban is felmerülő problémákhoz és eltérjenek az előző évektől. 2025-től a hadtáp, a katonai közlekedési és a haditechnikai specializáción kívül a gyakorlaton a katonai pénzügyi hallgatók is részt vesznek, akiknek szorosabb integrálása még a jövő feladatai közé tartozik.

A gyakorlat összekapcsolása a FOURLOG többnemzeti logisztikai kiképzéssel

A logisztikus tisztjelöltek szakmai pályára készítése során több egymásra épülő szakharcászati gyakorlaton és szakkiképzésen is részt vesznek. Ezeket az eseményeket az elméleti tudás megszerzését követően az ismeretek beágyazódását és gyakorlati végrehajtását elősegítendő szervezzük. Az előre tervezett kiképzési tevékenységek közül kiemelkedik a 6. félév során Tatán, a 7. szemeszter idején Táborfalván, végül pedig már a végzős tisztjelöltek záróvizsgáját megelőzően Ausztriában, Magyarországon és Csehországban levezetett FOURLOG Logisztikai Kiképzés.

Míg Tatán konkrét logisztikai tervezői feladatokat hajtanak végre, Táborfalván MEL-/MIL[26]-incidensekre reagálás során, úgynevezett „mini-törzsmunka" keretében végeznek szakmai tevékenységet a jövő logisztikus tisztjei. Az utolsó nagy gyakorlati megmérettetés alatt pedig egy fiktív szcenárió nyújtja azt a hátteret, amely meghatározza a szintén hallgatói csoportokban végrehajtandó munkát. Ekkor már a tervezési tevékenységekhez nélkülözhetetlen, korábbi tanulmányaik során elsajátított adatelemzői, -feldolgozói, kockázatelemzői és összességében analitikus gondolkodást igénylő képességeiket is fel kell használniuk a feladatok megoldásához. A gyakorlati kiképzésnek tükröznie kell a jelen kor biztonsági és katona logisztikai kihívásait, illetve az ezekre adandó válaszokat tartalmazó új koncepciók, szabályzók, eljárások és lehetséges megoldások tisztjelöltekkel történő megismertetését is. Az orosz–ukrán konfliktusból fakadó biztonsági fenyegetés, valamint ennek jellemzőiből jelentkező logisztikai kihívások miatt a többnemzeti műveletek során egyre nagyobb szerep hárul a BNT-re, illetve a polgári beszállítók szolgáltatásaira. Az ezekkel kapcsolatos nehézségeket, összetett támogatási folyamatokat a szervezők a FOURLOG Logisztikai Kiképzés során is igyekeznek modellezni. A tisztjelöltek számára a legnagyobb kihívás ekkor a rövid idő, ami a tervezői feladatok elvégzésére rendelkezésre áll. A műveleti terület megismerése, a szcenárió részleteinek megértése és a nemzetközi munkacsoportok katonáinak eltérő ismeretanyagbeli, illetve nyelvi képességeinek különbségeiből adódó eltérések áthidalása mellett a logisztikai folyamatok gyakorlati végrehajtásának és egymásra épülő logikai rendszerének helyes alkalmazása is elvárt tőlük. Ez utóbbi alatt értjük a gyakorlat során a lövészzászlóaljakat játszó munkacsoportok által végrehajtandó szükségletek meghatározását, az így nyert információk alapján a *szükségleti jegyzék* helyes elkészítését (*statement of requirement,* SOR), majd az igények és az információk megfelelő kommunikálását a Nemzeti Támogató

[26] MEL MIL, *main events list/main incidents list.*

Elemet megszemélyesítő másik tervezői csoport felé. Ez a team pedig a szükségletek kielégítéséhez elengedhetetlen források beazonosítását, a szolgáltatások és anyagok beszerzési árának megállapítását kell hogy elvégezze, javaslatot téve a beszállító kiválasztására. A 2024-ben végrehajtott FOURLOG-kiképzés alatt egyértelművé vált,[27] hogy a fenti tevékenységet és munkafolyamatot már korábbi kiképzések során is el kell kezdeni begyakoroltatni a tisztjelöltekkel, hogy ne nemzetközi környezetben szembesüljenek először ennek a tevékenységsorozatnak a kihívásaival. Ezért úgy döntöttünk, hogy ez is bekerül a 2025-ös táborfalvai szakharcászati gyakorlatba. Mivel ebben az esetben a hadszíntéren jellemzően pénzügyi tiszt által végzett beszerzéssel kapcsolatos munkáról van szó, első ízben bevontuk a katonai pénzügyi specializáció végzős hallgatóit is. Mindezt több okból is hasznosnak tartottuk; mert:

- gyakorlati formában is lehetőségük van a helyi beszerzés előkészítési folyamatainak fejlesztésére;
- az így nyert jártasság alapot jelenthet az MH missziós területen végzendő beszerző tiszti vagy a többnemzeti műveletekben gyakran megjelenő beszerző tiszt képviselője *(contracting officer's representative)* beosztás tevékenységének megismeréséhez;
- a szükségleti jegyzék helyes elkészítésén keresztül az igények pontos kommunikálásában, valamint a logisztikai koordinációs folyamatokban rutint szerezhetnek. Ez a precíz szakmai munka elvégzése mellett a koordináció fontosságának hangsúlyozására is remek alkalmat biztosít. Ezért a logisztikai és pénzügyi szakterületek hatékony együttműködésének begyakorlása, már a rendelkezésre álló szakmai tudás birtokában, mindenképp indokolt volt a 7. félévben megrendezett gyakorlaton is.

A két szakterület együttműködésére és gyakorlati feladatuk végrehajtására nagyjából az volt a jellemző, mint a fentebb már említett, tavalyi FOURLOG-gyakorlaton tapasztaltakra. Vagyis hogy a logisztikai tisztjelöltek ugyan meglehetősen pontosan elkészítették a szükségleti jegyzéket, de a megfelelő anyagok és szolgáltatások beszerzéséhez már nem szolgáltattak elegendő vagy elég részletes információt a pénzügyes (beszerző) tiszti hallgatóknak. Megjegyezzük, hogy tapasztalataink szerint ez gyakran megfigyelhető a valós katonai beszerzések esetén is, amikor többéves tapasztalattal rendelkező tisztek és főtisztek követnek el hasonló hibát. Sőt, a probléma az International Security Assistance Forces (ISAF) parancsnokságán Kabulban szolgáló COR-tiszt és a NATO-szerződés integrátor szervezete közötti szakmai együttműködés kapcsán is előjött, vagyis a két fél közti kooperáció nem hozta meg a várt eredményt, aminek következményeként az International Board of Auditors for NATO (IBAN) a kiképzés fontosságát emelte ki a Supreme Headquarters of Allied Power Europe (SHAPE) számára írt jelentésében.[28]

Az igények megfogalmazása és kommunikálása alatt jelentkező félreértések és pontatlanságok kiküszöbölésére több lehetőség is adott. A legkézenfekvőbb a szoros együttműködés és koordináció a két szereplő (az igénytámasztó és a beszerző) között,

[27] Szajkó–Pap–Gulyás 2024.
[28] North Atlantic Council 2015.

hogy minden részlet, minőség, mennyiség és szolgáltatási időintervallum precízen meghatározott legyen a beszerzési eljárás megkezdése előtt. Ezt az erőfeszítést aláásha tja, ha az igénytámasztó (jelen esetben a gyakorlaton a logisztikai szakág) maga sem tudja a szükséges részletességgel és pontossággal leírni, hogy mire van szüksége, mivel felmerülhet, hogy a kielégítendő igény meglehetősen komplex. Ez a probléma viszont kezelhető, ha a leggyakrabban előforduló anyag- és szolgáltatásigényekre vonatkozóan szükségletijegyzék-mintákat alkalmazunk. Az MH is készített ilyen segédletként szolgáló dokumentumokat, ezeket azonban érdemes tovább bontani, illetve kiegészíteni további szempontokkal és adatokkal, hogy még részletesebb mintaokmányok álljanak rendelkezésre. Ennek elkészítéséhez támaszkodhatunk korábbi igények elemzéseire és saját tapasztalatainkra is. Ez utóbbival viszont a tisztjelöltek még nem rendelkeznek.

Így fordult elő, hogy miután a logisztikus honvéd tisztjelöltek nem a szükséges alapossággal kommunikálták a beszerzendő anyagokat és szolgáltatásokat, a pénzügyes tisztjelöltek bizonyos igényelemeket kihagytak a piaci szereplőktől bekért ajánlatokból. Ez nyilvánvalóan képesség- vagy kapacitáshiányt okozna egy helytelen adatok alapján levezetett beszerzési eljárást követően – ami a szerződés módosítását vonná maga után –, vagy az ajánlati felhívás javítását eredményezné. Valószínűleg mindkét esetben megtörténne a tervezett határidők csúszása.

Jelen szakharcászati gyakorlaton a fenti problémák miatt a pénzügyes hallgatók nem mindig a kívánt anyagra vagy szolgáltatásra határoztak meg beszerzési költségeket, amelyeknek a megállapítását egyébként nyílt forrásból (elektronikus úton vagy telefonos piackutatás révén) hajtották végre. A hallgató zászlósok több piaci szereplő szolgáltatásait is beazonosították, így a szükséges anyagok és szolgáltatások kiválasztásához opcionális lehetőségeket dolgoztak ki a potenciális beszállítók árainak, szolgáltatásainak előnyeivel és hátrányaival együtt. A rendelkezésre álló információk alapján képesek voltak a megjelenített követelmények kielégítése érdekében hozzájárulni a parancsnok döntésének előkészítéséhez.

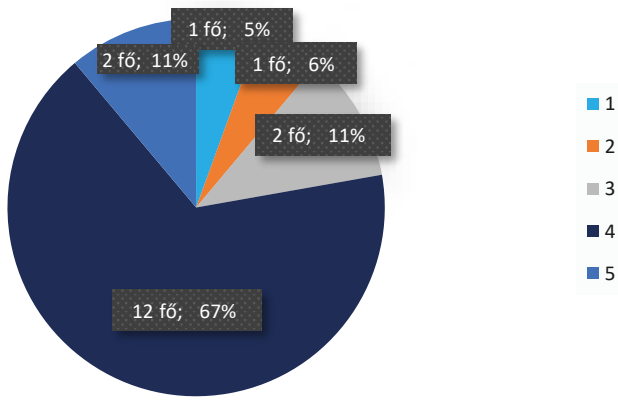
A gyakorlat végén végrehajtott tapasztalatfeldolgozás alatt egyértelművé váltak a tisztjelöltek által elkövetett hibák és a megfelelő koordináció fontossága is. Az a tény, hogy az említett szakágak közötti együttműködést már a 7. félévi kiképzési eseményen gyakorolhatták a tisztjelöltek, jó esélyt biztosít arra, hogy az egyetemi képzésük utolsó gyakorlatán ezen hibák kiküszöbölésére több figyelmet fordítsanak. Végeredményben pedig, hogy tiszti karrierjük során tisztában legyenek a beszerzési eljárások előkészítése folyamán rendkívül fontos, precíz szükségleti jegyzék elkészítésének, illetve az együttműködő szervezetekkel történő megfelelő koordináció és kommunikáció végrehajtásának jelentőségével.

A szakharcászati gyakorlat végrehajtásának tapasztalatai

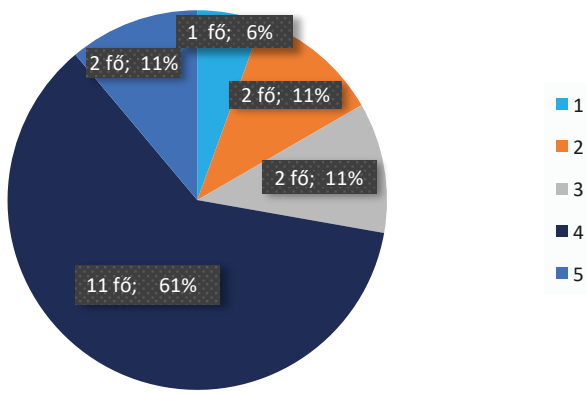
Hasonlóan a FOURLOG 2024 Logisztikai Kiképzés tapasztalataihoz,[29] az 5 napos foglalkozás végén a gyakorlat vezetőjével értékeltük a honvéd tisztjelöltek munkáját

[29] Szajkó–Pap–Gulyás 2024.

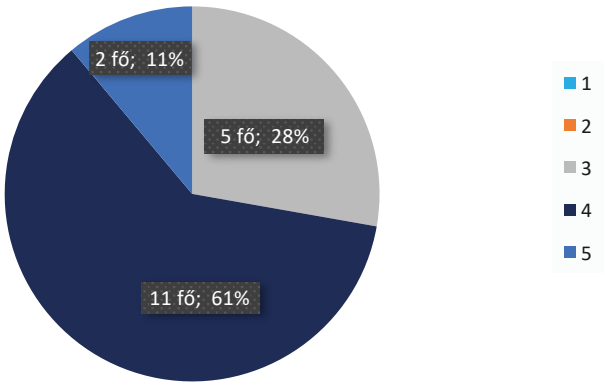
és teljesítményét, valamint felhívtuk a hibákra a figyelmet, majd a honvéd tisztjelöltek kitöltöttek egy kérdőívet, amely a felkészítő időszaktól kezdve a befejezésig, továbbá a valós logisztikai támogatásra vonatkozóan is tartalmazott kérdéseket. Ezek eredményét a következő ábrákban szemléltettük, külön fázisokra bontva. Az előkészítő időszakra feltett kérdések és a hallgatói válaszok a 3–5. ábrákon láthatók. Az értékelés során ötfokozatú skálán minősíthettek a honvéd tisztjelöltek.



3. ábra: A feladat értelmezése, tisztázása az oktatói állomány részéről a hallgatók részére
Forrás: a szerzők szerkesztése a kérdőív alapján



4. ábra: Az oktatók által rendelkezésre bocsátott irodalom, dokumentáció használhatósága
Forrás: a szerzők szerkesztése a kérdőív alapján



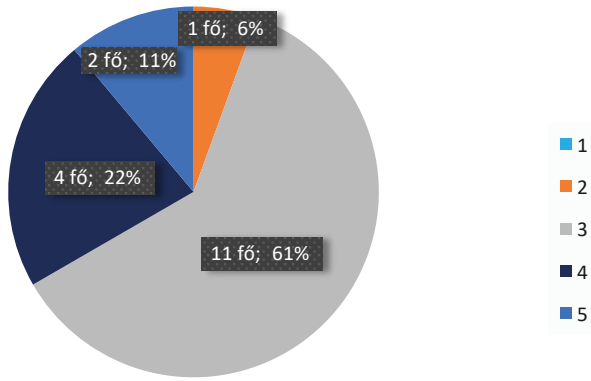
5. ábra: Az oktatók tevékenysége a gyakorlatra való felkészítés időszakában
Forrás: a szerzők szerkesztése a kérdőív alapján

A hallgatók mind tanóra, mind pedig konzultáció formájában minden segítséget megkaptak a gyakorlat előkészítésének időszakában, amely a válaszadók (18 fő) 80–90%-ának véleménye szerint is így volt. Az értékelésből az is kitűnik, hogy nem minden kitöltő volt elégedett maradéktalanul a felkészítéssel, valószínűleg ez annak köszönhető, hogy a katonai pénzügyi specializációs honvéd tisztjelöltek most először vettek részt a szakharcászati foglalkozáson, mert eddig ők ebben az időintervallumban már csapatgyakoroltatáson voltak.

A tényleges végrehajtás során első alkalommal fordult elő, hogy csak szemrevételezni mentünk ki (eddig minden évben a gyakorlat teljes időtartama alatt ott tartózkodtunk) a honvéd tisztjelöltekkel az MH Anyagellátó Raktárbázis Bázisparancsnokság Táborfalva Petőfi Laktanyájába (MH ARB BPTF),[30] mert az Adaptive Hussars 2025 hazai rendezésű, nagy láthatóságú nemzetközi gyakorlat miatt a laktanya területén is folytak honvédségi feladatok ebben az időszakban, amelyen később az oktatók is részt vettek.

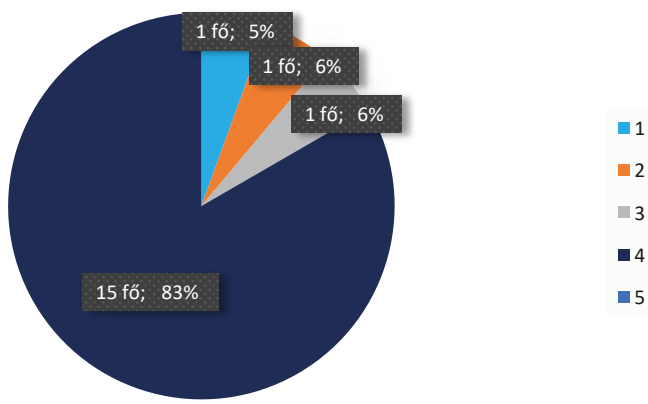
A végrehajtás fázisával kapcsolatban megfogalmazott kérdéseket és válaszokat a 6–10. számú ábrák szemléltetik. A válaszokat ötfokozatú skálában helyeztük el.

[30] Jelenlegi szervezeti megnevezés, korábban MH KKK Közlekedési Anyagraktár.

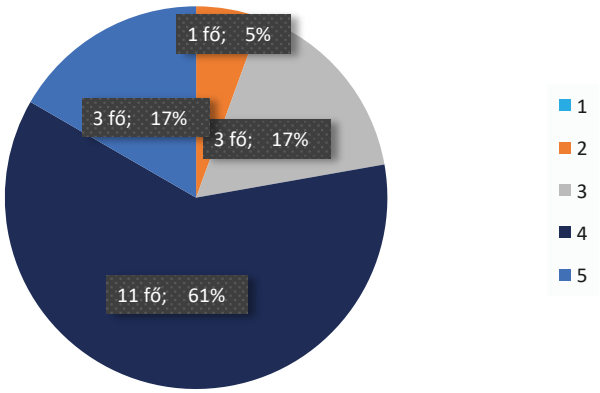


6. ábra: A kiadott feladat érthetősége
Forrás: a szerzők szerkesztése a kérdőív alapján

A 6. ábra értékeléséből látható, hogy 1 fő kivételével mindenki 3-as, vagy a fölötti minősítést adott, tehát a hallgatók megértették a kiadott feladatot, amely illeszkedett a korábban, több tantárgy keretében tanított elméleti ismeretekhez. A számottevő 3-as osztályzat oka lehetett, hogy a gyakorlathoz szükséges ismeretek a hallgatók számára nem álltak össze rendszerré, vagy az idő múlásával azok „megkoptak". A kidolgozás során többször felmerültek olyan problémák, amelyekre a megoldást kis rávezetéssel meg tudták találni, mert az adott témáról az oktató már a tanórán beszélt (7. ábra).



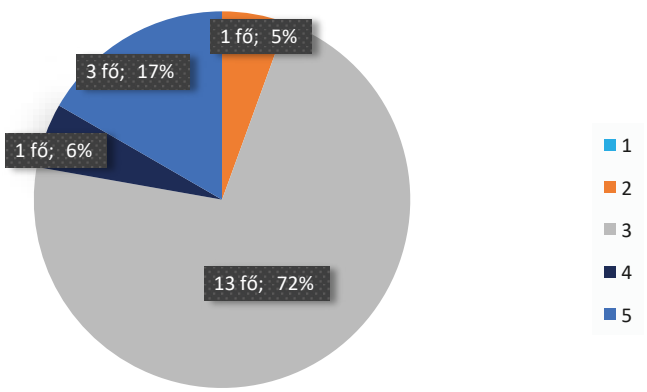
7. ábra: A kiadott feladatok illeszkedése a korábban oktatott ismeretekhez
Forrás: a szerzők szerkesztése a kérdőív alapján



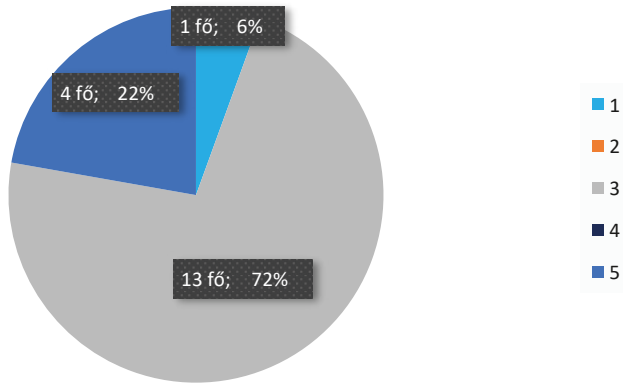
8. ábra: Az oktatók által meghatározott/hallgatók által választott törzsmunkamódszer hatékonysága
Forrás: a szerzők szerkesztése a kérdőív alapján

A honvéd tisztjelöltek részéről a feladatok kidolgozásához választott törzsmunkamódszer hatékonysága megfelelő volt, amelyet a 8. ábra szemléltet.

A 9. ábrát vizsgálva látható, amit már feljebb is írtunk (felkészülés ADHU-ra), hogy az oktatók nem mindig tudtak mindannyian egyszerre ott tartózkodni a kapott feladatok megoldása során, ezért közreműködésük a kidolgozásban nem tudott maradéktalanul hozzájárulni a sikeresebb végrehajtáshoz, amit a 10. ábra eredménye is mutat.



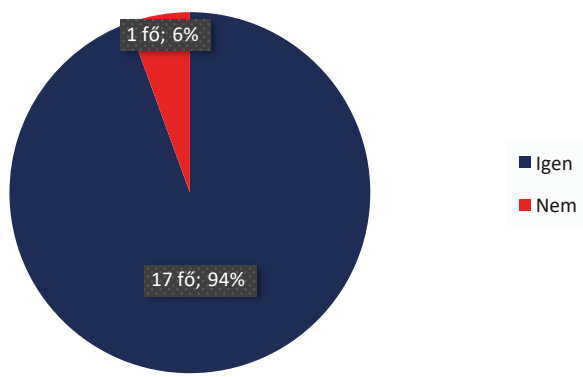
9. ábra: A beosztott segítő oktató(k) hozzájárulása a feladat sikeres megoldásához
Forrás: a szerzők szerkesztése a kérdőív alapján



10. ábra: A gyakorlatvezető tevékenységének értékelése
Forrás: a szerzők szerkesztése a kérdőív alapján

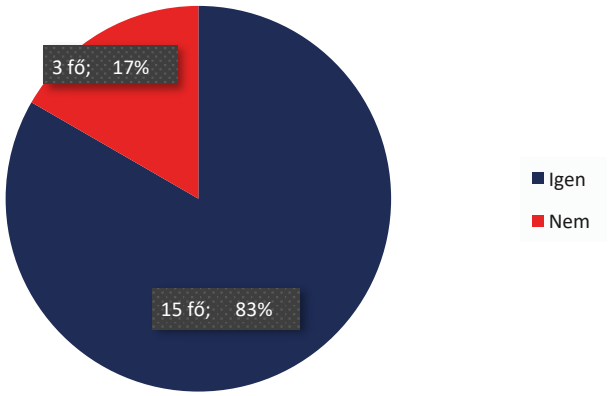
Összességében a válaszokból kitűnik, hogy a hallgatók túlnyomó többségben az 5 kérdés esetében (6–10. ábrák) a 3-as és 4-es „osztályzatot" adták a válaszokra, amely véleményünk szerint azzal függ össze, hogy a gyakorlatot követő héttől az oktatók is részt vettek az ADHU 2025 gyakorlaton, és emiatt folyamatosan anyagokat kellett felvenniük vagy felkészítésre kellett menniük, így egyszerre mindhárman nem minden esetben voltak jelen. Ha összehasonlítjuk ezt a FOURLOG 2024 gyakorlat eredményeivel,[31] ahol az oktatóknak 100%-ban csak erre kellett koncentrálni, a hallgatói pozitív elégedettség szembetűnő.

A befejező (értékelő) időszak kérdései és válaszai a 11–16. ábrákon láthatók. Az értékelés során csak az igen/nem válaszok közül lehetett választani. Az első két értékelés egyértelmű (11–12. ábrák), míg a 3–5. kérdésekre (13–15. ábrák) a hallgatók kissé ellentmondásos értékelést adtak, holott ezek szorosan összefüggenek.

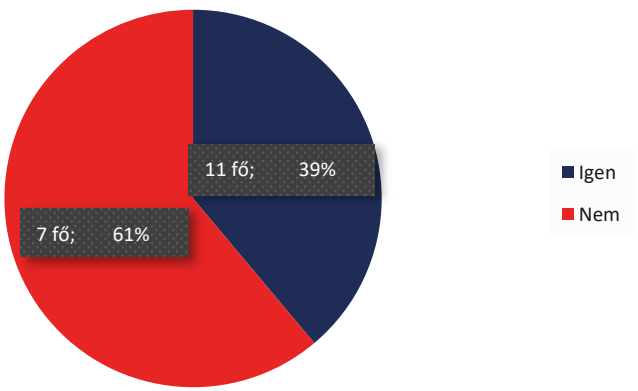


11. ábra: Történt-e gyakorlatvezetői értékelés a hallgatók számára?
Forrás: a szerzők szerkesztése a kérdőív alapján

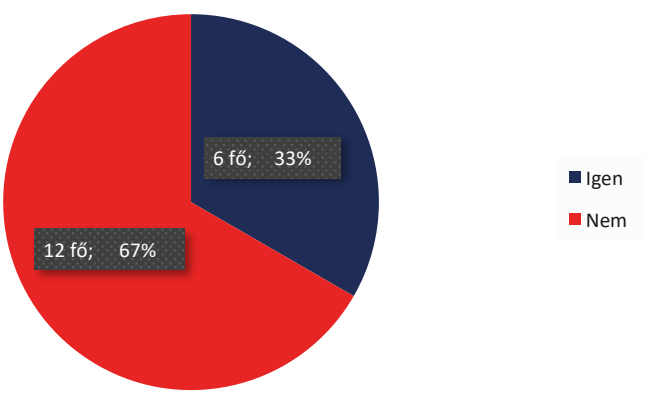
[31] Szajkó–Pap–Gulyás 2024.



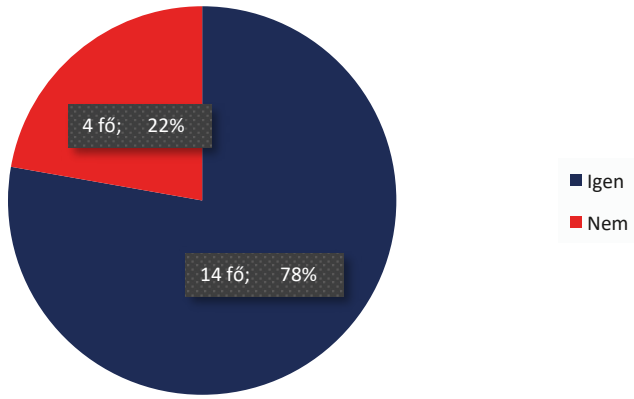
12. ábra: Hozzájárult-e a gyakorlat általános katonai szakmai ismereteinek bővítéséhez?
Forrás: a szerzők szerkesztése a kérdőív alapján



13. ábra: Hozzájárult-e a gyakorlat a harcászati szintű szakmai ismereteik bővítéséhez?
Forrás: a szerzők szerkesztése a kérdőív alapján



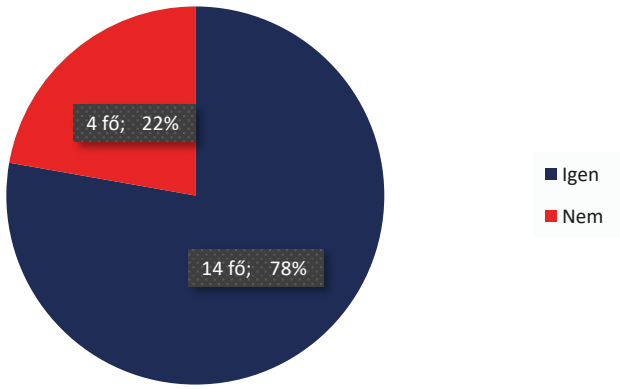
14. ábra: Hozzájárult-e a gyakorlat a harcászati szintű (logisztikai) törzsmunka, valamint az egyes törzsfunkciók együttműködésének megértéséhez és elsajátításához?
Forrás: a szerzők szerkesztése a kérdőív alapján



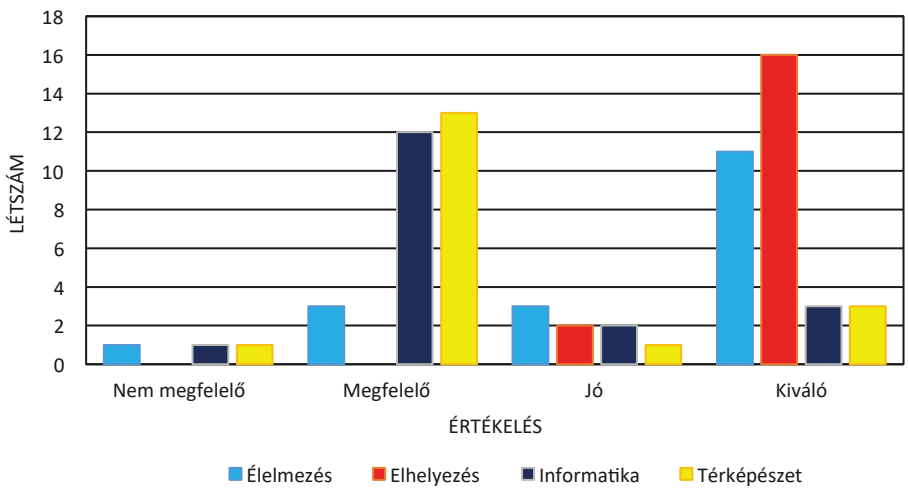
15. ábra: Hozzájárult-e a gyakorlat a műveleti parancsnoki lánc működésének, valamint a harcoló, harctámogató, harci kiszolgáló támogató erők, a befogadó nemzet és a polgári beszállítók kapcsolatának és együttműködésének megismeréséhez és megértéséhez?
Forrás: a szerzők szerkesztése a kérdőív alapján

A 16. ábra szemlélteti az egynapos, terepen történő szemrevételezés értékelését, amely nem minden honvéd tisztjelölt szerint segítette elő a tervezési feladatok sikeres végrehajtását. Nagy valószínűséggel azok a honvéd tisztjelöltek adták ezen válaszokat, akiknek a feladata az volt, hogy készítsenek pénzügyi elemzést (ehhez nem szükséges kivonulni terepre) a konvojtámogató központ működésének várható költségeiről az igénybevétel tervezett időtartamára, amelyhez a hadtápos, a közlekedési és a haditechnikai specializációs zászlósoknak kellett szolgáltatni az információkat. Ha ezek nem megfelelők vagy félreérthetők, akkor a kapott adatok nem teszik lehetővé a pontos költségtervezést, amire a gyakorlat értékelése során ki is tértünk.

A valós logisztikai biztosítással kapcsolatos kérdés az élelmezés, az elhelyezés, az informatika és a térképészet területekre terjedtek ki, ezt a 17. ábra szemlélteti, ahol a nem megfelelő, a megfelelő, a jó és a kiváló értékelés alapján hajthatták végre a honvéd tisztjelöltek az értékelést. Összességében elmondható, hogy a hallgatók (1 fő kivételével) elégedettek voltak a részükre biztosított logisztikai támogatással. Talán az élelmezési ellátás mutatja a legnagyobb szórást, amely véleményünk szerint nem indokolt, hiszen a hallgatók a gyakorlati időszakon kívüli időben is ezen étlap alapján fizetnek be az ebédre, ráadásul most térítésmentesen, természetbeni ellátásként járt nekik. Az informatikai és a térképészeti területre adott válaszok is elgondolkodtatók, mert a saját eszközüket használták a kidolgozáshoz az egyetemi wifihálózaton keresztül, amelyet az elmúlt években fejlesztettek. Az interneten elérhető digitális térképek pedig elegendők voltak a feladatuk elvégzéséhez.



16. ábra: Hozzájárult-e a helyszíni szemrevételezés a tervezési feladatok sikeres végrehajtásához?
Forrás: a szerzők szerkesztése a kérdőív alapján



17. ábra: Milyennek ítéli meg a gyakorlat valós logisztikai támogatását?
Forrás: a szerzők szerkesztése a kérdőív alapján

Összegzés

A katonai műveletek sikerének egyik alapfeltétele, hogy a kijelölt erők és hadfelszerelések a megfelelő időben, minőségben és mennyiségben érkezzenek meg a műveleti területre. Az orosz–ukrán fegyveres konfliktus miatt a NATO kiemelt figyelmet fordít az RSOM-képességek fejlesztésére, amelyek biztosítják a többnemzeti erők gyors

és hatékony bevethetőségét az európai hadszíntéren. Magyarország szerepe ebben a folyamatban a BNT rendszerén keresztül jelenik meg főként, amelynek működését több nagy volumenű gyakorlat, így a Saber Guardian 2017 és 2019 során is tesztelték.

A tanulmány alapján elmondható, hogy a tisztjelöltek felkészítése és oktatása csak akkor lehet eredményes, ha az elméleti képzés szervesen kiegészül olyan, egymásra épülő gyakorlati kiképzési programokkal, amelyek valós műveleti környezetet modelleznek. A táborfalvai szakharcászati kiképzés tervezése során az egyik fontos cél az volt, hogy olyan feladatokat integráljunk a gyakorlat dokumentumaiba a sikeres megvalósításhoz (például a levezetési tervbe, a harcparancsba, a MEL/MIL-listába), amelyek igazodnak a napjainkban jelentkező katonai logisztikai kihívásokhoz. Ennek megfelelően a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar katonai logisztika alapképzési szakon kialakított RSOM-orientált képzési elemek bevezetése szükségszerű és indokolt lépés volt, és hozzájárul a tisztjelöltek gyakorlatorientált felkészítéséhez.

A honvéd tisztjelölti visszacsatolások fontosak a képzési folyamat fejlesztése szempontjából, mivel közvetlen információt szolgáltatnak az oktatás hatékonyságáról és relevanciájáról. Az ilyen jellegű értékelések lehetővé teszik, hogy az oktatók azonosítsák az erősségeket, valamint azokat a területeket, ahol fejlesztésre van szükség. A visszajelzések rendszerszintű feldolgozása hozzájárul és lehetőséget biztosít egy adaptív, folyamatosan megújuló képzési struktúra kialakításához. Ez különösen fontos a katonai felsőoktatásban, ahol a képzési tartalomnak és módszereknek folyamatosan igazodniuk kell a változó műveleti és szakmai követelményekhez. Mindezek alapján a hallgatói vélemények bevonása elengedhetetlen a képzés minőségének hosszú távú fenntartásához és fejlesztéséhez. A gyakorlat befejezését követően kérdőíves felmérést végeztünk a hallgatók körében, amelynek eredményei igazolják a képzés létjogosultságát, ugyanakkor rámutatnak bizonyos fejlesztési területekre is (például fontos, hogy a gyakorlatot tervező és szervező oktatók a kiképzés teljes időszakában elérhetők legyenek, és ne vonják be őket más feladatokba). Erősíteni szükséges továbbá a képzés során a hallgatók rendszerben való gondolkodását, hogy a tantárgyak során elsajátított ismereteket egységben tudják kezelni és megértsék az azok között lévő kapcsolatokat, összefüggéseket.

Összességében megállapítható, hogy az RSOM-műveletek oktatásának további erősítése, valamint a gyakorlati elemek bővítése hosszú távon növeli a tisztképzés hatékonyságát, valamint elősegítheti a küldetésorientált vezetési képesség kialakítását.

Felhasznált irodalom

Kolonics Attila (2018): Konvojtámogató Központ kialakítása Befogadó Nemzeti Támogatás keretében. *Honvédségi Szemle,* 146(3), 117–128. Online: https://honvedelem.hu/files/files/110428/hsz_2018_3_beliv_117_128.pdf

Magyar Róbert (2022): Az összhaderőnemi támogatás új szervezeti egysége és annak feladatai a NATO-ban. *Honvédségi Szemle,* 150(2), 3–20. Online: https://doi.org/10.35926/HSZ.2022.2.1

NATO SHAPE (2024): *Criteria and Standards for the Zones of the Reinforcement and Sustainment Network.* Mons. NATO
NATO Standardization Agency (2014): *ATP-3.13.1 (STANAG 2580) Reception, Staging and Onward Movement (RSOM) Procedures, Edition A Version 1.*
NATO Standardization Agency (2018): *AJP-4.6 Allied Joint Doctrine for Joint Logistic Support Group, Edition C Version 1 (Draft)*.
NATO Standardization Agency (2025): *AJP-4 Allied Joint Doctrine for Sustainment of operations Edition C Version 1 (Draft).*
North Atlantic Council (2015): *IBAN Special Report to Council on the Steps Needed to Improve ACO and NSPA Management of Contractor Support to Operations.* Online: www.nato.int/content/dam/nato/webready/documents/iban/performance-audits/150720-aco-nspa-eng.pdf
Pete Szabolcs (2019): A mozgáskoordináló központ működése a befogadó nemzeti támogatás keretén belül. *Honvédségi Szemle,* 147(4), 114–133. Online: https://real.mtak.hu/125226/1/HSZ_2019_147_4_Pete_Szabolcs.pdf
Szajkó Gyula – Pap Andrea – Gulyás György (2024): A FOURLOG 2024 logisztikai kiképzés magyarországi szakaszának tapasztalatai és újszerű elemei. *Hadmérnök,* 19(3), 67–83. Online: https://doi.org/10.32567/hm.2024.3.5
Venekei József – Szajkó Gyula (2020): Magyarország lehetséges szerepe a NATO RSOM-műveleteiben. *Hadtudományi Szemle,* 13(4), 23–40. Online: https://doi.org/10.32563/hsz.2020.4.3

Egyéb források

144/2017. számú HVKF parancs a „SABER GUARDIAN 2017" nemzetközi gyakorlat és kapcsolódó nemzeti gyakorlatok előkészítéséről, valamint a „SABER GUARDIAN 2017" gyakorlat végrehajtásával kapcsolatos nemzeti támogatási feladatok végrehajtásáról
62/2017 MH LK PK parancs a „SABER GUARDIAN 2017" nemzetközi gyakorlat és kapcsolódó nemzeti gyakorlatok végrehajtásával kapcsolatos logisztikai támogatási feladatok végrehajtásáról

Melléklet

Kérdőív a Szakharcászati felkészítés értékeléséhez (2025 Táborfalva)						
I. Felkészítési időszak	**Értékelés**					**Összesen**
	1	**2**	**3**	**4**	**5**	
1. A feladat értelmezése, tisztázása az oktatói állomány részéről a hallgatók részére	1	1	2	12	2	18
2. Az oktatók által rendelkezésre bocsátott irodalom, dokumentáció használhatósága	1	2	2	11	2	18
3. Az oktatók tevékenysége a gyakorlatra való felkészítés időszakában	0	0	5	11	2	18
II. Végrehajtási időszak						
1. A kiadott feladat érthetősége	0	1	11	4	2	18
2. A kiadott feladatok illeszkedése a korábban oktatott ismeretekhez	1	1	1	15	0	18
3. Az oktatók által meghatározott/ hallgatók által választott törzsmunka-módszer hatékonysága	0	1	3	11	3	18
4. A beosztott segítő oktató(k) hozzájárulása a feladat sikeres megoldásához	0	1	13	1	3	18
5. A gyakorlatvezető tevékenységének értékelése	1	0	13	0	4	18

III. Befejező időszak	**Értékelés**		**Összesen**
	Igen	**Nem**	
1. Történt-e gyakorlatvezetői értékelés a hallgatók számára?	17	1	18
2. Hozzájárult-e a gyakorlat általános katonai szakmai ismereteinek bővítéséhez?	15	3	18
3. Hozzájárult-e a gyakorlat a harcászati szintű szakmai ismereteinek bővítéséhez?	7	11	18
4. Hozzájárult-e a gyakorlat a harcászati szintű (logisztikai) törzsmunka, valamint az egyes törzsfunkciók együttműködésének megértéséhez és elsajátításához?	6	12	18
5. Hozzájárult-e a gyakorlat a műveleti parancsnoki lánc működésének, valamint a harcoló, harctámogató, harci kiszolgáló támogató erők, a befogadó nemzet és a polgári beszállítók kapcsolatának és együttműködésének megismeréséhez és megértéséhez?	14	4	18
6. Hozzájárult-e a helyszíni szemrevételezés a tervezési feladatok sikeres végrehajtásához?	14	4	18

7. Milyennek ítéli meg a gyakorlat valós logisztikai támogatását?	**Nem megfelelő**	**Megfelelő**	**Jó**	**Kiváló**	**Összesen**
Élelmezés	1	3	3	11	18
Elhelyezés	0	0	2	16	18
Informatika	1	12	2	3	18
Térképészet	1	13	1	3	18

Tartalom